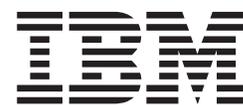


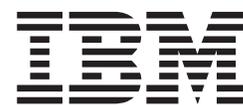
Nways Multiprotocol Access Services



Guía del usuario de software

Versión 3.4

Nways Multiprotocol Access Services



Guía del usuario de software

Versión 3.4

Nota

Antes de utilizar este documento, lea la información general que encontrará en la sección "Avisos" en la página xxvii.

Segunda edición (octubre de 1999)

Este manual es la traducción del original inglés *Nways Multiprotocol Access Services Software User's Guide Version 3.4 (SC30-3886-06)*.

Esta edición se aplica a la Versión 3 Release 4 de IBM Nways Multiprotocol Access Services y a todos los releases y modificaciones subsiguientes hasta que se indique lo contrario en nuevas ediciones o boletines técnicos.

Solicite las publicaciones al representante de IBM o en la sucursal de IBM de su localidad. Las publicaciones no están almacenadas en la dirección que se indica más abajo.

IBM agradece sus comentarios. Al final de esta publicación, encontrará una hoja de comentarios del lector. Si ya se ha utilizado, puede dirigir sus comentarios a:

IBM S.A.
National Language Solutions Center
Avda. Diagonal 571, Edif. "L'Illa"
08029 Barcelona
España

Además, puede enviar los comentarios sobre la documentación, así como otra información de soporte del producto en la Web:

<http://www.networking.ibm.com/support/docs.nsf>

Quando se envía información a IBM, se otorga un derecho no exclusivo de usar o distribuir la información en la manera en que se crea adecuada sin incurrir en ninguna obligación con el remitente.

© Copyright International Business Machines Corporation 1997, 1999. Reservados todos los derechos.

Contenido

Figuras	xxiii
Tablas	xxv
Avisos	xxvii
Marcas registradas	xxix
Prefacio	xxxi
Quién debe leer este manual	xxxi
Obtención de información adicional	xxxi
Acerca del software	xxxi
Convenios utilizados en este manual	xxxii
Visión general de la biblioteca	xxxiii
Resumen de los cambios para la biblioteca de software del IBM 2216.	xxxv
Network Utility	xxxvi
Funciones de software soportadas por Network Utility	xxxvii

Parte 1. Comprensión y utilización del software 1

Capítulo 1. Introducción	3
Antes de empezar	3
Migración al release actual	3
Acceso al software mediante consolas locales y remotas	3
Consolas locales.	3
Consolas remotas	4
Inicio de sesión remota o localmente	5
Volver a cargar el dispositivo	6
Salir del dispositivo	6
Explicación del sistema de interfaces del usuario	6
Comprensión de la interfaz de usuario de primer nivel	6
Capítulo 2. Utilización del software	9
Entrada de mandatos	9
Conexión a un proceso	9
Identificación de los indicadores	10
Cómo obtener ayuda.	10
Cómo salir de un entorno de nivel inferior	11
Volver a OPCON	11
Algunas sugerencias sobre la configuración	11
Creación de una primera configuración	11
Basar una configuración en una configuración existente.	12
Acceso a los procesos de segundo nivel	14
Acceso al proceso de configuración, CONFIG (Talk 6)	14
Acceso al proceso de operación/supervisión de la consola, GWCON (Talk 5)	15
Acceso al proceso de consola ELS secundario, ELSCON (Talk 7)	15
Acceso a los procesos de tercer nivel	16
Adición de dispositivos	16
Acceso a los procesos de configuración y operación de características	21
Acceso a los procesos de configuración y operación de protocolos.	22
Finalización del mandato	23
Ayuda en línea cuando la finalización de mandatos está habilitada.	24
Ayuda en línea cuando la finalización de mandatos está inhabilitada	26

Histórico de mandatos	27
Repetición de un mandato del Histórico de mandatos	27
Repetición de una serie de mandatos del Histórico de mandatos	28
Capítulo 3. Acceso al firmware desde la interfaz de línea de mandatos	31
Acceso al indicador del firmware	31
Opciones de arranque disponibles para el 2216	31
Modalidad atendida	32
Modalidad autónoma	32
Capítulo 4. Proceso y mandatos OPCON	33
¿Qué es el proceso OPCON?	33
Acceso al proceso OPCON	33
Mandatos OPCON	33
Configuration	34
Console	34
Diags	35
Divert	35
Els	36
Event	36
Flush	36
Halt	37
Intercept	37
Logout	37
Memory	38
Ping	38
Reload	39
Status	40
Suspend	41
Talk	41
Telnet	42

Parte 2. Comprensión, configuración y utilización de los servicios básicos . . . 45

Capítulo 5. Utilización de BOOT Config para efectuar la gestión de cambios	47
Comprensión de la gestión de cambios	47
Utilización de Trivial File Transfer Protocol (TFTP)	47
Transferencia de grandes cantidades de datos a múltiples archivos	48
Especificación del número máximo de bloques que se han de transferir a un archivo del receptor	48
Carga de una imagen a una hora específica	49
Capítulo 6. Configuración de la gestión de cambios	51
Acceso al entorno de configuración de la gestión de cambios	51
Mandatos de configuración de la gestión de cambios	51
Add	52
Copy	52
Describe	54
Disable	55
Enable	55
Erase	56
List	57
Lock	58
Set	59
TFTP	60

Timeload	61
Unlock	63
Update-firmware	64
Capítulo 7. El proceso CONFIG (CONFIG - Talk 6) y sus mandatos	67
¿Qué es CONFIG?	67
Modalidad de Sólo configuración	67
Configuración rápida	69
Configuración del acceso de usuario	70
Configuración de interfaces de repuesto	71
Restablecimiento de interfaces	74
Utilización de vuelcos del sistema	75
Entrada y salida de CONFIG	76
Mandatos CONFIG	76
Add	77
Boot	84
Change	84
Clear	91
Delete	93
Disable	94
Enable	95
Event	96
Feature	96
List	97
Load	101
Network	102
Patch	102
Performance	105
Protocol	105
Qconfig	106
Set	106
Recuperación del sistema	112
System View	113
Time	114
Unpatch	115
Update	115
Write	115
Capítulo 8. El proceso de operación/supervisión (GWCON - Talk 5) y sus mandatos	117
¿Qué es GWCON?	117
Entrada y salida de GWCON	117
Mandatos GWCON	118
Activate	118
Buffer	119
Clear	120
Configuration	120
Disable	123
Disk	124
Enable	124
Error	125
Event	126
Feature	126
Interface	126
Memory	127
Network	129

Performance	130
Protocol	130
Queue	130
Reset	131
Statistics	132
Test	132
Uptime	133
Capítulo 9. El proceso de gestión de mensajes (MONITR - Talk 2)	135
¿Qué es la gestión de mensajes (MONITR)?	135
Mandatos que afectan a la gestión de mensajes	135
Entrada y salida del proceso de gestión de mensajes (MONITR)	135
Recepción de mensajes	135
Capítulo 10. Utilización del Sistema de anotación cronológica de sucesos (ELS)	137
¿Qué es ELS?	137
Entrada y salida del entorno de configuración ELS	138
Conceptos de la anotación cronológica de sucesos	138
Causas de los sucesos	138
Interpretación de un mensaje	139
Utilización de ELS	141
Gestión de la rotación de mensajes ELS	142
Captura de la salida ELS utilizando una conexión Telnet en un sistema principal UNIX	142
Configuración de ELS para que los mensajes de sucesos se envíen en rupturas SNMP	143
Utilización de ELS para resolver un problema	143
Ejemplo 1 de ELS	144
Ejemplo 2 de ELS	144
Ejemplo 3 de ELS	144
Utilización y configuración de la anotación cronológica remota ELS	145
Recurso y nivel de la anotación cronológica del sistema	145
Configuración de una estación de trabajo remota	146
Configuración del 2216 para la anotación cronológica remota	147
Salida de la anotación cronológica remota	149
Consideraciones adicionales	152
Utilización de almacenamiento intermedio de mensajes ELS	153
Capítulo 11. Configuración y supervisión del Sistema de anotación cronológica de sucesos (ELS)	157
Acceso al entorno de configuración ELS	157
Mandatos de configuración ELS	157
Add	158
Advanced	158
Clear	158
Default	159
Delete.	159
Display	159
Filter	160
List	160
Nodisplay	162
Noremote	162
Notrace	164
Notrap	164
Remote	165

Set	167
Trace	172
Trap	173
Mandatos de configuración de filtros de red ELS	173
Mandatos de configuración de almacenamiento intermedio de mensajes ELS.	176
Entrada y salida del entorno operativo ELS	180
Mandatos de supervisión ELS	180
Advanced	181
Clear	181
Display	182
Files Trace TFTP	182
Filter	183
List.	183
Nodisplay	185
Noremote	186
Notrace	187
Notrap	187
Packet Trace	188
Remote	188
Remove	190
Restore	191
Retrieve	191
Save	191
Set	191
Statistics.	197
Trace	199
Trap	200
View	201
Mandatos de supervisión de rastreo de paquetes.	201
Mandatos de la supervisión de filtros de red ELS.	204
Mandatos de la supervisión de almacenamientos intermedios de mensajes ELS.	206
Capítulo 12. Configuración y supervisión del rendimiento	213
Visión general del rendimiento.	213
Exactitud de la información del rendimiento	213
Acceso al entorno de configuración del rendimiento	213
Mandatos de configuración del rendimiento	214
Disable	214
Enable	214
List.	214
Set.	214
Acceso al entorno de supervisión del rendimiento	215
Mandatos de supervisión del rendimiento.	215
Disable	215
Enable	215
List.	216
Report	216
Set.	216

Parte 3. Comprensión, configuración y funcionamiento de las interfaces 217

Capítulo 13. Iniciación a las interfaces de red	219
Antes de continuar	219
Interfaces de red y el mandato interface de GWCON	219

Acceso a los procesos de configuración y de consola de interfaces de red	219
Acceso a los procesos de configuración y de consola de protocolos de capa de enlace	220
Definición de interfaces de repuesto	220
Capítulo 14. Configuración de interfaces de Red en Anillo IEEE 802.5	221
Acceso al proceso de configuración de interfaces de Red en Anillo	221
Mandatos de configuración de Red en Anillo	221
List.	221
LLC	222
Media	222
Packet-Size	223
Set	223
Source-routing	224
Speed.	224
Acceso al proceso de supervisión de interfaces	224
Mandatos de supervisión de interfaces de Red en Anillo	225
Dump	225
LLC	226
Interfaces de Red en Anillo y mandato interface de GWCON	226
Estadísticas visualizadas para las interfaces de Red en Anillo 802.5.	226
Soporte para la reconfiguración dinámica de Red en Anillo	229
Delete Interface de CONFIG (Talk 6)	229
Activate Interface de GWCON (Talk 5).	229
Reset Interface de GWCON (Talk 5)	230
Capítulo 15. Configuración y supervisión de la Red en Anillo Rápida	231
Acceso al proceso de configuración de interfaces FasTR	231
Mandatos de configuración FasTR	231
List.	232
LLC	232
Media	232
Packet-Size	232
Set	233
Source-routing	233
Speed.	234
Acceso al proceso de supervisión de interfaces	234
Mandatos de supervisión de la interfaz FasTR	234
Dump	234
LLC	235
Interfaces FasTR y mandato interface de GWCON	235
Estadísticas visualizadas para las interfaces FasTR	235
Capítulo 16. Utilización de FDDI	239
Visión general de Fiber Distributed Data Interface (FDDI)	239
Red en anillo de paso de señales	239
Anillos primarios y secundarios	239
Conexión de dispositivos.	239
Diferencias entre FDDI y Red en Anillo	240
Clases de dispositivos A y B	240
Diagrama de red FDDI	241
Capítulo 17. Configuración y supervisión de FDDI	243
Acceso a los mandatos de configuración FDDI.	243
Mandatos de configuración FDDI.	243
List.	243

LLC	244
Set	244
Acceso a los mandatos de supervisión FDDI	246
Mandatos de supervisión FDDI	246
List	246
LLC	246
Srt-stat	246
Interfaces FDDI y el mandato GWCON	247
Estadísticas visualizadas desde interfaces FDDI	247
Capítulo 18. Configuración y supervisión de interfaces LLC	251
Acceso al proceso de configuración de interfaces	251
Mandatos de configuración LLC	251
List	252
Set	252
Acceso al proceso de supervisión de interfaces	254
Mandatos de supervisión LLC	255
Clear-Counters	255
List	255
Set	261
Capítulo 19. Utilización de la interfaz de red Ethernet	263
Visualización de estadísticas Ethernet mediante el mandato interface	263
Capítulo 20. Configuración y supervisión de la interfaz de red Ethernet	267
Acceso al proceso de configuración de interfaces Ethernet	267
Mandatos de configuración Ethernet	267
Connector-Type	268
IP-Encapsulation	268
List	268
Physical-Address	268
Acceso al proceso operativo de la interfaz Ethernet	269
Mandatos de supervisión de interfaz Ethernet	269
Collisions	270
Soporte para la reconfiguración dinámica de Ethernet	270
Delete Interface de CONFIG (Talk 6)	270
Activate Interface de GWCON (Talk 5)	270
Reset Interface de GWCON (Talk 5)	271
Capítulo 21. Utilización de la interfaz de red Ethernet de 10/100 Mbps	273
Visualización de estadísticas Ethernet de 10/100 Mbps	273
Negociación automática en la interfaz Ethernet de 10/100 Mbps	281
Configuración de valores distintos de automático para dúplex	281
Configuraciones que pueden resultar en una anomalía de la activación del enlace en el IBM 2216	281
Configuraciones que pueden resultar en discrepancias de las modalidades de dúplex durante el funcionamiento	282
Capítulo 22. Configuración y supervisión de la interfaz de red Ethernet de 10/100 Mbps	285
Acceso al proceso de configuración de interfaces	285
Mandatos de configuración de Ethernet de 10/100-Mbps	285
Duplex	286
IP-Encapsulation	286
List	287
Physical-Address	287

Speed.	288
Acceso al proceso de supervisión de interfaces Ethernet	288
Mandatos de supervisión de la interfaz Ethernet de 10/100 Mbps	289
Collisions	289
Soporte para la reconfiguración dinámica de Ethernet	289
Delete Interface de CONFIG (Talk 6)	290
Activate Interface de GWCON (Talk 5)	290
Reset Interface de GWCON (Talk 5)	290
Capítulo 23. Visión general de LAN Emulation	291
Beneficios de LAN Emulation	291
Componentes de LAN Emulation	292
Direccionamiento en ATM	293
ESI	294
Direcciones ATM de componentes de LAN Emulation	294
Visión general de las funciones de ILMI relacionadas	295
Configuración manual de la versión de señalización	295
Localización de LECS utilizando ILMI	295
Visión general de la función LECS	296
Situaciones de ejemplo de utilización de las políticas de asignación del LECS	298
Más información acerca de los parámetros TLV	300
Conexión al LES	300
Registro de direcciones	301
Resolución de direcciones	301
Conexión al BUS	302
Funciones del BUS	302
Establecimiento de una VCC de datos directos	303
Visión general de extensiones para LAN Emulation	304
Broadcast Manager	304
Soporte BCM para IP	304
Soporte BCM para IPX	305
Soporte BCM para NetBIOS	305
Soporte de BCM para el puente de ruta de origen	306
Fiabilidad de LAN Emulation	306
Seguridad de LAN Emulation	308
Interfaz de red a red de LAN Emulation (LNNI)	309
Parámetros clave de configuración para LAN Emulation	309
Capítulo 24. Utilización de ATM	311
ATM y LAN Emulation	311
Cómo entrar direcciones	311
Multiplexación ATM-LLC	312
Conceptos de interfaz virtual ATM	312
Ventajas de utilizar las interfaces virtuales ATM	312
Desventajas de utilizar las interfaces virtuales ATM	313
Capítulo 25. Configuración y supervisión de ATM	315
Acceso al proceso de configuración de la interfaz ATM	315
Mandatos de configuración ATM	315
Mandatos de configuración de interfaces ATM	316
Add	317
List	317
QoS Configuration	317
Remove	318
Set	318

Enable	321
Disable	322
Acceso al proceso de configuración de interfaz virtual ATM	322
Mandatos de configuración de interfaz virtual ATM	322
Add	323
List	323
Remove	323
Acceso al proceso de supervisión de ATM	323
Mandatos de supervisión ATM	324
Interface	324
ATM-LLC	324
Mandatos de supervisión de la interfaz ATM (indicador ATM INTERFACE+)	325
List	325
Trace	326
Wrap	327
Mandatos de supervisión ATM-LLC	327
List	328
Mandatos de supervisión de interfaz virtual ATM	328
Soporte para la reconfiguración dinámica de ATM y ATM virtual	328
Delete Interface de CONFIG (Talk 6)	328
Activate Interface de GWCON (Talk 5)	328
Reset Interface de GWCON (Talk 5)	329
Capítulo 26. Utilización de los LAN Emulation Client	331
Visión general de LAN Emulation Client	331
Capítulo 27. Configuración y supervisión de LAN Emulation Clients	333
Configuración de los clientes de emulación de LAN	333
Add	333
Config.	334
List	334
Remove	334
Configuración de un LE Client conforme a ATM Forum	334
ARP Configuration	335
Frame	337
IP-Encapsulation (sólo para los LEC Ethernet conformes a ATM Forum)	338
List	339
LLC	339
QoS	339
RIF-Timer (sólo para los LEC conformes a Token-Ring Forum)	339
Set	340
Source-Routing (sólo para los LEC conformes a Token-Ring Forum)	350
Mandatos de configuración LLC	351
List	351
Set	351
Acceso al entorno de supervisión del LEC	353
Mandatos de supervisión del LEC	353
List	354
LLC	357
MIB	358
QoS Information	362
Trace	362
Mandatos de supervisión LLC	363
List	363
Set	363
Soporte para la reconfiguración dinámica de LEC	364

Delete Interface de CONFIG (Talk 6)	364
Activate Interface de GWCON (Talk 5)	364
Reset Interface de GWCON (Talk 5)	365
Mandatos de cambio temporal de GWCON (Talk 5)	365
Capítulo 28. Utilización de adaptadores de canal	367
Planificación de la definición de sistema principal	367
Definición de IOCP para el 2216	368
Definición del 2216 en el sistema operativo	372
Definición del 2216 en programas del sistema principal	374
Planificación para el soporte de 2216	387
Análisis y resolución de problemas de adaptador de canal del 2216	388
Reconfiguración	388
Visión general del adaptador de canal	388
Soporte de estación de canal LAN (LCS)	391
Soporte de Link Services Architecture (LSA)	394
Soporte de canal de diversas vías de acceso+ (MPC+)	400
Configuración de la interfaz de adaptador de canal	407
Capítulo 29. Configuración y supervisión de los adaptadores de canal	
ESCON y paralelo	409
Acceso a la interfaz de canal	409
Mandatos de configuración de adaptador de canal	410
Add	411
Delete	426
Mod	426
List (ESCON)	429
List (PCA)	430
Set (sólo PCA)	430
Acceso al proceso de supervisión de interfaces de canal	431
Mandatos de supervisión de interfaces de canal	431
List	432
Net	434
Dump_adapter	435
HIDTrace	435
Trace	435
Tune	435
Mandatos de supervisión de interfaces LCS de adaptador de canal	436
List	436
Tune	438
Mandatos de supervisión de interfaces LSA de adaptador de canal	438
List	438
Tune	440
Mandatos de supervisión de interfaces MPC+ de adaptador de canal	441
List	441
Tune	446
Capítulo 30. Soporte para la reconfiguración dinámica del canal ESCON	447
Delete Interface de CONFIG (Talk 6)	447
Activate Interface de GWCON (Talk 5)	447
Reset Interface de GWCON (Talk 5)	447
Mandatos de cambio temporal de GWCON (Talk 5)	447
Capítulo 31. Soporte para la reconfiguración dinámica del canal PCA	449
Delete Interface de CONFIG (Talk 6)	449
Activate Interface de GWCON (Talk 5)	449

Reset Interface de GWCON (Talk 5)	449
Mandatos de cambio temporal de GWCON (Talk 5)	449
Capítulo 32. Soporte para la reconfiguración dinámica del canal virtual	
LSA	451
Delete Interface de CONFIG (Talk 6)	451
Activate Interface de GWCON (Talk 5)	451
Reset Interface de GWCON (Talk 5)	451
Mandatos de cambio temporal de GWCON (Talk 5)	452
Capítulo 33. Soporte para la reconfiguración dinámica del canal virtual	
LCS	453
Delete Interface de CONFIG (Talk 6)	453
Activate Interface de GWCON (Talk 5)	453
Reset Interface de GWCON (Talk 5)	453
Mandatos de cambio temporal de GWCON (Talk 5)	454
Capítulo 34. Soporte para la reconfiguración dinámica del canal virtual	
MPC	455
Delete Interface de CONFIG (Talk 6)	455
Activate Interface de GWCON (Talk 5)	455
Reset Interface de GWCON (Talk 5)	455
Mandatos de cambio temporal de GWCON (Talk 5)	456
Capítulo 35. Soporte para la reconfiguración dinámica de la interfaz de bucle de retorno APPN	
Delete Interface de CONFIG (Talk 6)	457
Activate Interface de GWCON (Talk 5)	457
Reset Interface de GWCON (Talk 5)	457
Capítulo 36. Configuración de interfaces de línea serie	
Acceso al proceso de configuración de interfaces	459
Cronometraje y tipo de cable	459
Interfaces de red y el mandato interface de GWCON	460
Capítulo 37. Utilización de la interfaz de red X.25	
Procedimientos de configuración básica	461
Establecimiento de la personalidad nacional	462
Comprensión de los valores por omisión de X.25	462
Encapsulación nula	464
Límites	464
Cambios de configuración	464
Configuración de encapsulación nula y Grupos de usuarios cerrados (CUG)	464
Comprensión de los grupos de usuarios cerrados	465
Grupos de usuarios cerrados bilaterales	466
Tipos de grupos de usuarios cerrados extendidos	466
Establecimiento de circuitos X.25 con grupos de usuarios cerrados en un dispositivo	466
Configuración de grupos de usuarios cerrados X.25	467
Capítulo 38. Configuración y supervisión de la interfaz de red X.25	
Mandatos de configuración X.25	469
Set	470
Enable	475
Disable	476
National Enable	476

National Disable	479
National Set	479
National Restore	484
Add	485
Change	492
Delete.	493
List.	494
Acceso al proceso de supervisión de interfaces	497
Mandatos de supervisión X.25.	497
List.	498
Parameters.	498
Reset	499
Statistics.	500
Interfaces de red X.25 y el mandato interface de GWCON	501
Estadísticas visualizadas para las interfaces X.25	501
Soporte de la reconfiguración dinámica de la interfaz de red X.25	504
Delete Interface de CONFIG (Talk 6)	504
Activate Interface de GWCON (Talk 5).	504
Reset Interface de GWCON (Talk 5)	504
Capítulo 39. Utilización de XTP	505
El X.25 Transport Protocol	505
Información de configuración	506
Comodines de dirección DTE	508
Función de similar de reserva XTP	508
Búsqueda de un DTE remoto	508
Temporizador de petición de conexión	509
XTP local	509
XTP y grupos de usuarios cerrados	509
Configuración de XTP	510
Procedimientos de configuración	510
Establecimiento del enlace de datos	511
Configuración de la interfaz IP.	512
Configuración de X.25.	512
Establecimiento de la personalidad nacional	513
Definición de la dirección IP	514
Establecimiento de la dirección IP interna	514
Configuración de XTP	514
Ejemplo de configuración de direccionadores remotos	516
Capítulo 40. Configuración y supervisión de XTP	519
Mandatos de configuración XTP	519
Add	519
Change	522
Delete.	522
Enable	524
Disable	524
Set	524
List.	524
Mandatos de supervisión XTP	526
Add	526
Delete.	527
List.	527
Soporte para la reconfiguración dinámica de la interfaz de red X.25	530
Delete Interface de CONFIG (Talk 6)	530
Activate Interface de GWCON (Talk 5).	530

Reset Interface de GWCON (Talk 5)	530
Capítulo 41. Utilización de interfaces Frame Relay	531
Visión general de Frame Relay	531
Red Frame Relay	532
Subinterfaces para Frame Relay	533
Circuitos virtuales conmutados Frame Relay	533
Manejador de tramas Frame Relay	534
Inicialización de la interfaz Frame Relay	535
Circuitos huérfanos	536
Configuración de los estados de PVC para que afecten al estado de la interfaz Frame Relay	537
Opción de interfaz de punto a punto	538
Trama Frame Relay	538
Reenvío de tramas a través de la red Frame Relay	540
Direcciones de protocolo	540
Emulación de multidifusión y difusión de protocolo	541
Gestión de la red Frame Relay	541
Informe del estado de la gestión	542
Informe de estado completo	542
Informe de verificación de la integridad del enlace	542
Gestión de capa de enlace consolidada (CLLM)	543
Velocidades de datos Frame Relay	543
Velocidad de información confirmada (CIR)	543
CIR de circuito virtual permanente huérfano	543
Tamaño de ráfaga confirmado (Bc)	544
Tamaño de exceso de ráfaga (Be)	544
Velocidad de línea	545
Velocidad mínima de información	545
Velocidad máxima de información	545
Velocidad variable de información	545
Congestión de circuitos	546
Supervisión de CIR	546
Supervisión de la congestión	547
Notificación y evitación de la congestión	547
Congestión del circuito Frame Handler	549
Supervisión de CIR	549
Supervisión de la congestión	550
Sin supervisión	550
Reserva de ancho de banda en Frame Relay	551
Fragmentación a través de una interfaz Frame Relay	551
Reenvío de voz a través de Frame Relay	552
Sugerencias para configurar el 2216 para VoFR	552
Configuración de interfaces Frame Relay	553
Configuración del BRS	557
Visualización del indicador de configuración de Frame Relay	558
Procedimiento de la configuración básica de Frame Relay	558
Habilitación de la gestión de PVC en Frame Relay	559
Habilitación de la gestión de SVC en Frame Relay	560
Capítulo 42. Configuración y supervisión de interfaces Frame Relay	561
Mandatos de configuración Frame Relay	561
Add	562
Change	571
Disable	572
Enable	576

List	583
LLC	591
Remove	592
Set	593
Acceso al indicador de supervisión de Frame Relay	600
Mandatos de supervisión Frame Relay	600
Clear	600
Disable	601
Enable	601
List	601
LLC	613
Notrace	613
Set	613
Trace	615
Interfaces Frame Relay y mandato interface de GWCON	615
Estadísticas visualizadas para las interfaces Frame Relay	615
Soporte para la reconfiguración dinámica de Frame Relay	617
Delete Interface de CONFIG (Talk 6)	618
Activate Interface de GWCON (Talk 5)	618
Reset Interface de GWCON (Talk 5)	618
Mandatos de cambio temporal de GWCON (Talk 5)	618
Capítulo 43. Utilización de interfaces de Point-to-Point Protocol	621
Visión general de PPP	621
Estructura de trama de capa de enlace de datos PPP	622
Link Control Protocol (LCP) de PPP	624
Paquetes LCP	625
Paquetes de establecimiento de enlace	626
Paquetes de terminación de enlace	627
Paquetes de mantenimiento de enlace.	628
Protocolos de autenticación de PPP	628
Password Authentication Protocol (PAP)	629
Challenge-Handshake Authentication Protocol (CHAP)	629
Autenticación Microsoft CHAP de PPP (MS-CHAP)	629
Shiva Password Authentication Protocol (SPAP)	630
Configuración de la autenticación PPP	630
Configuración de llamada de retorno PPP	631
Utilización de AAA con PPP	633
Network Control Protocol de PPP	633
AppleTalk Control Protocol	633
Banyan VINES Control Protocol	633
Bridging Control Protocol.	633
Callback Control Protocol	634
DECnet IV Control Protocol.	634
IP Control Protocol	634
IPv6 Control Protocol	635
IPX Control Protocol	635
OSI Control Protocol	636
APPN HPR Control Protocol	636
APPN ISR Control Protocol.	636
Utilización y configuración de conexiones virtuales	636
Consideraciones acerca de VC	636
Configuración de un VC	637
Capítulo 44. Configuración y supervisión de interfaces Point-to-Point Protocol	639

Acceso al proceso de configuración de interfaces	639
Acceso al indicador de configuración de interfaz PPP	639
Mandatos de configuración Point-to-Point.	640
Disable	640
Enable	642
List.	644
LLC	649
Set.	649
Acceso al proceso de supervisión de interfaces	661
Mandatos de supervisión Point-to-Point	662
Clear	662
List.	662
LLC	686
Interfaces Point-to-Point Protocol y el mandato interface de GWCON	686
Soporte para la reconfiguración dinámica de Point-to-Point Protocol	689
Delete Interface de CONFIG (Talk 6)	689
Activate Interface de GWCON (Talk 5).	689
Reset Interface de GWCON (Talk 5)	689
Capítulo 45. Utilización de Multilink PPP Protocol	691
Consideraciones acerca de MP	692
MP de múltiples chasis	693
Configuración de una interfaz Multilink PPP	693
Configuración de MP en circuitos de marcación PPP	693
Configuración de MP en enlaces serie PPP	694
Configuración de MP en redes con túneles de capa 2	694
Configuración de MP de múltiples chasis	695
Interposición de paquetes en Multilink PPP	696
Capítulo 46. Configuración y supervisión de Multilink PPP Protocol (MP)	697
Acceso al indicador de configuración MP	697
Mandatos de configuración MP para interfaces Multilink PPP	697
Disable	697
Enable	698
Encapsulator	698
List.	698
Set.	699
Supervisión del estado de interfaces MP	701
Acceso a los mandatos de supervisión MP	701
Mandatos de supervisión Multilink PPP Protocol	701
List.	701
Capítulo 47. Configuración y supervisión de SDLC Relay	707
Visión general de SDLC Relay	707
Procedimiento de configuración básica	709
Reconfiguración dinámica	709
Acceso al entorno de configuración SDLC Relay	709
Mandatos de configuración SDLC Relay	710
Add	710
Delete.	712
Disable	712
Enable	712
List (para red SRLY)	713
List (para el protocolo SDLC Relay).	714
Set.	715
Acceso al entorno de supervisión SDLC Relay.	717

Mandatos de supervisión SDLC Relay	718
Clear-Port-Statistics.	718
Disable	718
Enable	719
List.	719
Interfaces SDLC Relay y el mandato interface de GWCON	720
Soporte para la reconfiguración dinámica de SDLC Relay	720
Delete Interface de CONFIG (Talk 6)	721
Activate Interface de GWCON (Talk 5).	721
Reset Interface de GWCON (Talk 5)	721
Capítulo 48. Utilización de interfaces SDLC	723
Procedimiento de configuración básica	723
Configuración de interfaces de llamada de entrada SDLC conmutadas	723
Requisitos de configuración SDLC	724
Capítulo 49. Configuración y supervisión de interfaces SDLC	725
Acceso al entorno de configuración SDLC	725
Mandatos de configuración SDLC	726
Add	726
Delete.	728
Disable	728
Enable	728
List.	729
Set	732
Acceso al entorno de supervisión SDLC	739
Mandatos de supervisión SDLC	739
Add	740
Clear	740
Delete.	740
Disable	740
Enable	741
List.	741
Msgsz.	744
Set	744
Test	748
Interfaces SDLC y mandato interface de GWCON	749
Estadísticas visualizadas para interfaces SDLC	749
Capítulo 50. Utilización de la interfaz de red V.25bis	751
Antes de empezar	751
Procedimientos de configuración	751
Adición de direcciones V.25bis.	751
Configuración de la interfaz V.25bis	752
Adición de circuitos de marcación	753
Configuración de circuitos de marcación	753
Capítulo 51. Configuración y supervisión de la interfaz de red V.25bis	755
Acceso al proceso de configuración de interfaces	755
Mandatos de configuración V.25bis	755
List.	756
Set	757
Acceso al proceso de supervisión de interfaces	759
Mandatos de supervisión V.25bis.	760
Calls	760
Circuits	761

Parameters	762
Statistics	763
V.25bis y los mandatos GWCON	764
Estadísticas para las interfaces V.25bis y circuitos de marcación	765
Capítulo 52. Utilización de la interfaz RDSI	769
Visión general de RDSI	769
Adaptadores e interfaces RDSI	769
Circuitos de marcación	770
Direccionamiento	771
Exceso de suscripciones y contención de circuitos	771
Control del coste a través de circuitos a petición	771
ID y LIDS del llamador	772
Códigos de causa RDSI	772
Configuraciones RDSI de ejemplo	774
Configuración Frame Relay a través de RDSI	774
Configuración de Restauración de WAN	774
T1/E1 canalizado	775
Requisitos y restricciones para interfaces RDSI	776
Conmutadores/Servicios soportados	776
Restricciones de interfaz RDSI	776
Requisitos de configuración de circuitos de marcación	776
Antes de empezar	776
Procedimientos de configuración	777
Adición de direcciones RDSI	777
Configuración de parámetros RDSI	777
Configuración de la interfaz RDSI	778
Adición de circuitos de marcación	779
Configuración de circuitos de marcación	780
Variante de conmutador I.431	781
Soporte de I.431 nativo	781
Capítulo 53. Configuración y supervisión de la interfaz RDSI	783
Mandatos de configuración RDSI	783
Block-Calls	783
List	784
Remove	784
Set	784
Cause Code	788
Acceso al proceso de supervisión de interfaces	789
Mandatos de supervisión RDSI	789
Block-Calls	789
Calls	790
Channels	790
Circuits	790
Dial-dump	791
L2_Counters	792
L3_Counters	792
TEI	792
Parameters	792
Statistics	793
RDSI y los mandatos GWCON	793
Interfaz — Estadísticas para interfaces RDSI y circuitos de marcación	794
Configuración—Información sobre el hardware y el software del direccionador	795
Soporte para la reconfiguración dinámica de RDSI	795

Delete Interface de CONFIG (Talk 6)	795
Activate Interface de GWCON (Talk 5)	795
Reset Interface de GWCON (Talk 5)	795
Capítulo 54. Configuración y supervisión de circuitos de marcación	797
Mandatos de configuración de circuitos de marcación	797
Delete.	798
Encapsulator	798
List.	799
Set.	801
Mandatos de supervisión de circuitos de marcación	804
Callback	804
Soporte para la reconfiguración dinámica de circuitos de marcación	804
Delete Interface de CONFIG (Talk 6)	805
Activate Interface de GWCON (Talk 5)	805
Reset Interface de GWCON (Talk 5)	805

Parte 4. Apéndices 807

Apéndice A. Consulta para la configuración rápida	809
Consejos para la configuración rápida	809
Selecciones	809
Salida y Reinicio	809
Cuando haya terminado	810
Inicio del programa de Configuración rápida.	810
Configuración de LAN Emulation	810
Configuración de la función de puente	811
Configuración de protocolos	812
Configuración de IP.	813
Configuración de IPX	814
Configuración DECnet (DNA)	817
Volver a cargar el dispositivo	819
Apéndice B. Personalidades nacionales X.25	821
GTE-Telenet	821
DDN	821
Apéndice C. Creación de un archivo de carga del direccionador a partir de múltiples discos	823
Ensamblaje de un archivo de carga bajo DOS	823
Ensamblaje de un archivo de carga bajo UNIX.	823
Desensamblaje de un archivo de carga bajo DOS	824
Desensamblaje de un archivo de carga bajo UNIX	825
Apéndice D. Atributos remotos AAA.	827
Radius	827
Palabras clave	828
Ejemplo de archivo de configuración RADIUS	829
TACACS+	831
Lista de Abreviaturas	833
Glosario.	843
Índice.	871

Hoja de Comentarios	893
-------------------------------	-----

Figuras

1. Multiprotocol Access Services	7
2. Relación de los procesos y mandatos	8
3. Utilización de la memoria	38
4. Mensaje generado por un suceso	139
5. Descripción de mensajes de la anotación cronológica del sistema	145
6. Archivo de configuración syslog.conf	147
7. Configuración del 2216 para la anotación cronológica remota	148
8. Configuración de subsistemas y sucesos para la anotación cronológica remota	149
9. Contenido de ejemplo desde el archivo de información de noticias de la anotación cronológica del sistema	150
10. Salida de Talk 2.	151
11. Ejemplo del contenido del archivo <i>Syslog_user_alert</i>	151
12. Ejemplo de configuración de una entrada ARP estática	152
13. Ejemplo de números de secuencia repetidos en la salida de la anotación cronológica del sistema	153
14. Diagrama de red FDDI	241
15. Vistas física y lógica de una red sencilla de LAN Emulation	292
16. Conexiones por omisión entre clientes LE Client y el LES	301
17. Conexión por omisión entre clientes LE (LEC) y el BUS	302
18. Redundancia de LAN Emulation.	307
19. Ejemplo de configuración de canal ESCON	368
20. Ejemplo de configuración de sistema principal EMIF	370
21. Ejemplo de configuración de adaptador de canal paralelo	371
22. 2216 conectado a un sistema principal mediante un adaptador de canal ESCON/PCA - Vista lógica	389
23. Manejadores de red virtual del 2216 para LCS y LSA	390
24. Manejadores de red virtual del 2216 para MPC+.	391
25. Configuración de los manejadores de red virtual de Estación de canal LAN (LCS)	391
26. Configuración de manejadores de red virtual de Link Services Architecture (LSA)	394
27. Configuración de manejadores de red virtual para la conexión LSA directa	395
28. Configuración de manejadores de red virtual para la conexión LSA APPN	396
29. Configuración de manejadores de red virtual para la conexión LSA DLSw	397
30. Configuración de manejadores de red virtual para la conversión local LSA DLSw	399
31. Diferentes tipos de conexiones MPC+	401
32. Configuración de manejadores de red virtual para APPN a través del Canal de diversas vías de acceso+ (MPC+)	402
33. Configuración de manejadores de red virtual para UDP+ a través de MPC+	403
34. Configuración de manejadores de red virtual para TCP/IP a través de MPC+	405
35. Encapsulación nula de grupo de usuarios cerrado	465
36. Configuración antes y después de XTP	506
37. Ejemplo de configuración XTP	511
38. Los DLCI en la red FR	532
39. Multiplexación de circuitos DTE y DCE	535
40. Los DLCI en la red Frame Relay	536
41. Circuito huérfano	537
42. Formato de trama Frame-Relay	538
43. Notificación de congestión y moderación de la velocidad.	548
44. Ejemplo de configuración VoFR	554
45. Ejemplos de enlaces de punto a punto	622
46. Estructura de trama PPP	623
47. Estructura de trama LCP (en el campo de información PPP)	625
48. MP de múltiples chasis	695
49. Ejemplo de una configuración SDLC Relay.	708

50. Configuración Frame Relay a través de RDSI	774
51. Utilización de RDSI para la Restauración de WAN	775

Tablas

1. Funciones de código soportadas en el 2216 Modelo 400 y en Network Utility	xxxvii
2. Procesos, su finalidad y mandatos para acceder a ellos	10
3. Arquitectura de red e interfaces soportadas	19
4. Mandatos OPCON	33
5. Mandatos de la Configuración de la gestión de cambios	51
6. Posibilidades de la Configuración rápida	69
7. Resumen de los mandatos CONFIG	76
8. Permiso de acceso	83
9. Números y nombres de las características del IBM 2216	97
10. Funciones adicionales proporcionadas por el mandato de establecer nivel de indicador	110
11. Valores por omisión y máximos para interfaces	111
12. Resumen de los mandatos GWCON	118
13. Niveles de anotación cronológica	139
14. Códigos de terminación de paquetes (códigos de error)	140
15. Resumen de los mandatos de configuración ELS	157
16. Mandatos de configuración de filtros de red ELS	174
17. Mandatos de configuración de almacenamiento intermedio de mensajes ELS	176
18. Resumen de los mandatos de supervisión ELS	180
19. Resumen de los mandatos de supervisión de rastreo de paquetes	201
20. Mandatos de la supervisión de filtros de red ELS	204
21. Mandatos de la supervisión de almacenamientos intermedios de mensajes ELS	206
22. Resumen de los mandatos de configuración PERF	214
23. Resumen de los mandatos de supervisión PERF	215
24. Resumen de los mandatos de configuración de Red en Anillo	221
25. Tamaños de paquete válidos de Red en Anillo 4/16	223
26. Resumen de los mandatos de supervisión de Red en Anillo	225
27. Resumen de los mandatos de configuración FasTR	231
28. Resumen de los mandatos de supervisión FasTR	234
29. Resumen de los mandatos de configuración FDDI	243
30. Resumen de los mandatos de supervisión FDDI	246
31. Resumen de los mandatos de configuración LLC	251
32. Resumen de los mandatos de supervisión LLC	255
33. Resumen de los mandatos de configuración de Ethernet	267
34. Resumen de los mandatos de supervisión Ethernet	269
35. Configuraciones que pueden resultar en anomalía de enlace en el IBM 2216	282
36. Configuraciones que pueden resultar en discrepancias de las modalidades de dúplex durante el funcionamiento	283
37. Resumen de los mandatos de configuración de Ethernet	285
38. Resumen de los mandatos de supervisión Ethernet	289
39. Resumen de los mandatos de configuración ATM	315
40. Resumen de los mandatos de configuración de interfaces ATM	316
41. Resumen de los mandatos de configuración de interfaz virtual ATM	322
42. Resumen de los mandatos de supervisión ATM	324
43. Resumen de los mandatos de supervisión de interfaces ATM	325
44. Resumen de los mandatos de configuración ATM LLC	327
45. Resumen de los mandatos de configuración de LAN EMULATION Client.	333
46. Resumen de los mandatos de configuración de LAN Emulation Client.	335
47. Resumen de los mandatos ARP Configuration de ATM LAN Emulation Client	335
48. Resumen de los mandatos ARP Config de ATM LAN Emulation Client.	336
49. Resumen de los mandatos LLC	351
50. Resumen de los mandatos de supervisión de LE Client	353
51. Resumen de los mandatos de supervisión LLC	363
52. Mandatos de configuración de interfaz de canal	410

53. Mandatos de supervisión de interfaces de canal	431
54. Mandatos de supervisión de interfaces LCS de adaptador de canal.	436
55. Mandatos de supervisión de interfaces LSA de adaptador de canal.	438
56. Mandatos de supervisión de interfaces MPC+ de canal	441
57. Mandato set	462
58. Parámetros de National Enable	463
59. Parámetros de National Set	463
60. Establecimiento de circuitos X.25 internos para grupos de usuarios cerrados	467
61. Resumen de los mandatos de configuración X.25	469
62. Velocidades de línea cuando se utiliza el cronometraje interno para interfaces 2216	473
63. Velocidades de línea cuando se utiliza el cronometraje externo para interfaces 2216	474
64. Ejemplo de definiciones de VC	474
65. Resumen de los mandatos de supervisión X.25	497
66. Resumen de los mandatos de configuración XTP	519
67. Resumen de los mandatos de supervisión XTP	526
68. Correlación de direcciones de protocolo	540
69. Datos generados por un puerto de voz	555
70. Opciones de gestión de Frame Relay.	559
71. Resumen de los mandatos de configuración de Frame Relay	561
72. Velocidades de línea cuando se utiliza el cronometraje interno para interfaces 2216	598
73. Velocidades de línea cuando se utiliza el cronometraje externo para interfaces 2216	598
74. Opciones de gestión de Frame Relay.	598
75. Unidades de retardo de transmisión y rango para la interfaz serie 2216	599
76. Resumen de los mandatos de supervisión Frame Relay	600
77. Códigos de paquetes LCP	625
78. Resumen de los mandatos de configuración Point-to-Point	640
79. Tipos de cables para interfaces 2216	652
80. Velocidades de línea cuando se utiliza el cronometraje interno para interfaces 2216	654
81. Velocidades de línea cuando se utiliza el cronometraje externo para interfaces 2216	654
82. Resumen de los mandatos de supervisión Point-to-Point.	662
83. Mandatos de configuración MP	697
84. Mandatos de supervisión MP	701
85. Resumen de los mandatos de configuración SDLC Relay	710
86. Tipos de cables para las interfaces 2216	715
87. Valores válidos para el tamaño de trama en el mandato set frame-size	716
88. Velocidades de línea cuando se utiliza el cronometraje interno para interfaces 2216	717
89. Velocidades de línea cuando se utiliza el cronometraje externo para interfaces 2216	717
90. Resumen de los mandatos de supervisión SDLC Relay	718
91. Resumen de los mandatos de configuración SDLC.	726
92. Tipos de cables para interfaces 2216	733
93. Valores válidos para el tamaño de trama en el mandato link frame-size	733
94. Velocidades de línea cuando se utiliza el cronometraje interno para interfaces 2216	737
95. Velocidades de línea cuando se utiliza el cronometraje externo para interfaces 2216	737
96. Resumen de los mandatos de supervisión SDLC	739
97. Resumen de los mandatos de configuración V.25bis	755
98. Resumen de los mandatos de supervisión V.25bis	760
99. Códigos de causa RDSI Q.931	773
100. Resumen de los mandatos de configuración RDSI	783
101. Resumen de los mandatos de códigos de causa de RDSI	788
102. Resumen de los mandatos de supervisión RDSI.	789
103. Resumen de los mandatos de configuración de circuitos de marcación	797
104. Resumen de los mandatos de configuración de circuitos de marcación	804

Avisos

Es posible que IBM no comercialice los productos, servicios o dispositivos que aparecen en este manual en otros países. Consulte el representante local de IBM para obtener información sobre los productos y servicios que se ofrecen en su área. Cualquier referencia a un producto, programa o servicio de IBM no pretende afirmar ni implicar que sólo pueda utilizarse el mencionado producto, programa o servicio de IBM. En su lugar, puede utilizarse cualquier producto, programa o servicio funcionalmente equivalente que no vulnere ninguno de los derechos de propiedad intelectual de IBM. Sin embargo, es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

IBM puede tener patentes o solicitudes de patentes pendientes que cubran temas tratados en este documento. La entrega de este documento no otorga ninguna licencia sobre estas patentes. Puede solicitar información sobre licencias a:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
Estados Unidos

Para solicitar información sobre licencias relacionadas con DBCS (doble byte), póngase en contacto con el Departamento de la propiedad intelectual de IBM de su país o envíe las consultas a:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japón

El párrafo siguiente no se aplica al Reino Unido ni a ningún otro país en el que estas declaraciones sean contrarias a la legislación local: INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL" SIN GARANTÍA DE NINGUNA CLASE, NI EXPRESA NI IMPLÍCITA, INCLUYENDO PERO SIN LIMITARSE A LAS GARANTÍAS IMPLÍCITAS DE LEGALIDAD, COMERCIALIZACIÓN O IDONEIDAD PARA UNA FINALIDAD DETERMINADA. Algunos países no permiten la limitación de responsabilidad de garantías expresas o implícitas en determinadas transacciones, por lo tanto, es posible que esta declaración no se aplique en su caso.

Marcas registradas

Los términos siguientes son marcas registradas de International Business Machines Corporation en los Estados Unidos y/o en otros países:

Advanced Peer-to-Peer Networking
APPN
eNetwork
IBM
OS/2
SecureWay
VTAM

Microsoft, Windows, Windows NT y el logotipo de Windows son marcas registradas de Microsoft Corporation.

UNIX es una marca registrada en los Estados Unidos y en otros países con licencia exclusiva de X/Open Company Limited.

NetView es una marca registrada de Tivoli Systems, Inc. en los Estados Unidos y/o en otros países.

Java y todas las marcas comerciales y logotipos basados en Java son marcas registradas de Sun Microsystems, Inc. en los Estados Unidos y/o en otros países.

Otros nombres de empresas, productos y servicios pueden ser marcas registradas o de servicio de terceros.

Prefacio

Este manual contiene la información que necesitará para utilizar la interfaz de usuario del direccionador para configurar y utilizar el código base de Multiprotocol Access Services instalado en el dispositivo Nways. Con ayuda de este manual, podrá realizar los procesos y operaciones siguientes:

- Configurar, supervisar y utilizar el código base de Multiprotocol Access Services.
- Configurar, supervisar y utilizar las interfaces y el software de Capa de enlace soportados por el dispositivo Nways .

Este manual es el primer volumen de la biblioteca de software para el 2216, que se describe en la sección “Visión general de la biblioteca” en la página xxxiii. Puede que un dispositivo Nways específico no soporte todas las características y funciones descritas en la biblioteca. Si una característica o función es específica de un dispositivo, se indica esta restricción en el manual relevante o se muestra en una tabla en el prefacio de este manual.

Este manual hace referencia al 2216 como “el direccionador” o como “el dispositivo”. Los ejemplos de la biblioteca representan la configuración de un 2216, pero la salida real que se produzca puede variar. Utilice los ejemplos como directrices de lo que aparecerá cuando configure su dispositivo.

Quién debe leer este manual

Este manual está dirigido para las personas que instalan y gestionan redes de sistemas. Aunque la experiencia con el hardware y software de red de sistemas es de utilidad, no necesita tener experiencia como programador para utilizar el software de protocolo.

Obtención de información adicional

Pueden efectuarse cambios en la documentación después de que se impriman los manuales. Si está disponible información adicional o son necesarios cambios después de que se hayan impreso los manuales, encontrará los cambios en un archivo (denominado README) en el CD-ROM. Podrá visualizar el archivo con un editor de texto de código ASCII.

Acerca del software

IBM Nways Multiprotocol Access Services es el software que da soporte al IBM 2216 (número de programa bajo licencia 5765-C90). Este software tiene los componentes siguientes:

- El código base, que está compuesto por:
 - El código que proporciona las funciones de direccionamiento, puente, conmutación del enlace de datos y agente de SNMP para el dispositivo.
 - La interfaz de usuario de direccionador, que permite configurar, supervisar y utilizar el código base de Multiprotocol Access Services instalado en el dispositivo. Se accede a la interfaz de usuario de direccionador localmente mediante un terminal o emulador ASCII conectado al puerto de servicio o bien remotamente mediante un dispositivo conectado a un módem o una sesión Telnet.

El código base viene instalado de fábrica en el 2216.

- El Programa de configuración para IBM Nways Multiprotocol Access Services (denominado en este manual: *Programa de configuración*) es una interfaz gráfica de usuario que permite configurar el dispositivo desde una estación de trabajo autónoma. El Programa de configuración incluye la función de comprobación de errores e información de ayuda en línea.

El Programa de configuración no viene precargado de fábrica; se suministra separadamente del dispositivo como parte del pedido de software.

También puede obtener el Programa de configuración para IBM Nways Multiprotocol Access Services en la página de presentación. Consulte el manual *Guía del usuario del Programa de Configuración para productos Nways Multiprotocol y Access Services*, GC10-3430, para obtener la dirección del servidor y los directorios.

Convenios utilizados en este manual

En este manual se utilizan los siguientes convenios para mostrar la sintaxis de los mandatos y las respuestas de programa:

1. El formato abreviado de un mandato va subrayado de la manera mostrada en el ejemplo siguiente:

```
reload
```

En este ejemplo, puede entrar el mandato al completo (reload) o la abreviatura del mismo (rel).

2. Las opciones de palabra clave para un parámetro van entre corchetes y separadas por la palabra "o". Por ejemplo:

```
mandato [palabraclave1 o palabraclave2]
```

Elija una de las palabras clave como valor del parámetro.

3. Tres puntos a continuación de una opción tienen el significado de que se entran datos adicionales (por ejemplo, una variable) después de la opción. Por ejemplo:

```
time host ...
```

En este ejemplo, se entra la dirección IP del sistema principal en lugar de los puntos, tal como se explica en la descripción del mandato.

4. En la información visualizada como respuesta a un mandato, los valores por omisión para una opción van entre corchetes inmediatamente después de la opción. Por ejemplo:

```
Media (UTP/STP) [UTP]
```

En este ejemplo, el soporte de almacenamiento toma por omisión el valor de UTP a menos que se especifique STP.

5. Las combinaciones de teclas del teclado se indican en el texto de la manera siguiente:

- **Control-P**
- **Control -**

La combinación de teclas **Control -** indica que debe pulsar simultáneamente la tecla Control y el guión. En determinadas circunstancias, esta combinación de teclas cambia el indicador de línea de mandatos.

6. Los nombres de las teclas del teclado que se pulsan se indican así: **Intro**
7. Las variables (es decir, nombres utilizados para representar datos que define el usuario) aparecen en letra cursiva. Por ejemplo:

Visión general de la biblioteca

Cambios en la estructura de la biblioteca: A partir de la Versión 3.2, han tenido lugar los siguientes cambios en la organización de la biblioteca:

- La parte titulada **Comprensión, uso y configuración de las características** ha pasado de formar parte del manual *Utilización y configuración de las características* a formar parte del manual *Nways Multiprotocol Access Services Guía del usuario de software*.
- Los capítulos sobre el uso, la configuración y la supervisión de la característica DIALs se han incluido en el manual *Utilización y configuración de las características*.

Actualizaciones y correcciones de la información: Para mantenerse informado de los cambios técnicos, aclaraciones y arreglos implementados después de la impresión de los manuales, consulte las páginas de presentación del IBM 2216 en: <http://www.networking.ibm.com/216/216prod.html>

La lista siguiente muestra los manuales de la biblioteca de IBM 2216 agrupados según las tareas.

Planificación

GA27-4105

IBM 2216 Introduction and Planning Guide

Este manual se suministra con el IBM 2216. Explica cómo prepararse para la instalación y cómo llevar a cabo una configuración inicial.

Instalación

GA27-4106

IBM 2216 Nways Multiaccess Connector Installation and Initial Configuration Guide

Este manual se suministra con el IBM 2216. Explica cómo instalar el IBM 2216 y cómo verificar su instalación.

GX27-3988

2216 Nways Multiaccess Connector Hardware Configuration Quick Reference

Esta tarjeta de referencia se utiliza para entrar y guardar la información de configuración de hardware que se utiliza para determinar el estado correcto de un IBM 2216.

Diagnósticos y mantenimiento

SY27-0350

2216 Nways Multiaccess Connector Service and Maintenance Manual

Este manual se suministra con el IBM 2216. Proporciona instrucciones para diagnosticar problemas del IBM 2216 y repararlo.

Gestión de red y operaciones

La lista siguiente muestra los manuales que dan soporte al Multiprotocol Access Services.

SC10-3434

Guía del usuario de software

En este manual se explica cómo:

- Configurar, supervisar y utilizar el software de Multiprotocol Access Services.
- Utilizar la interfaz de usuario de direccionador de línea de mandatos de Multiprotocol Access Services para configurar y supervisar las interfaces de red y los protocolos de capa de enlace suministrados con IBM 2216.

SC10-3429

Utilización y configuración de las características

SC10-3432

Consulta de configuración y supervisión de protocolos Volumen 1

SC10-3433

Consulta de configuración y supervisión de protocolos Volumen 2

Estos manuales describen cómo acceder y utilizar la interfaz de usuario de línea de mandatos de Multiprotocol Access Services para configurar y supervisar el software de protocolo de direccionamiento que se ha suministrado con el producto.

Incluyen información sobre cada uno de los protocolos a los que dan soporte los dispositivos.

SC10-3431

Guía de mensajes del sistema para el registro cronológico de sucesos

Este manual contiene un listado de los códigos de error que pueden producirse así como las descripciones y las acciones recomendadas para corregir los errores.

Configuración**GC10-3430**

Guía del usuario del Programa de Configuración para productos Nways Multiprotocol y Access Services

Este manual describe cómo utilizar el Programa de Configuración.

Seguridad**SD21-0030**

Caution: Safety Information—Read This First

Este manual, suministrado con el IBM 2216, proporciona traducciones de avisos y peligro aplicables a la instalación y al mantenimiento de un IBM 2216.

Marketing

La página web de IBM proporciona información sobre el producto:

<http://www.networking.ibm.com/216/216prod.html>

Resumen de los cambios para la biblioteca de software del IBM 2216

La lista siguiente se aplica a los cambios que se han efectuado en el software de la Versión 3 Release 4:

- Mejoras en Frame Relay:
 - Nuevo soporte de Manejador de tramas (FH)
 - Regulación de PU para manejar las ráfagas de tráfico como soporte de los controladores 3745
 - Nuevo tipo de interfaz (subinterfaz Frame Relay) para permitir interfaces virtuales en la misma interfaz física
 - Soporte IP sin numerar
- Mejoras en VPN:
 - Mejoras en CPE:
 - La información de la política de los servidores LDAP se almacena localmente.
 - Configuración rápida de la política.
 - Comprobación de la coherencia de la política.
 - Ahora, puede recuperarse la información de la política de los servidores LDAP de un dominio de administración.
 - Ejecución de ping en túnel IPSec.
 - Mejoras en IP:
 - Mejoras en el direccionamiento de voz:
 - Compresión de cabeceras IP en PPP (RFC 2507, 2508, 2509)
 - Interposición del tráfico de voz entre paquetes de datos fragmentados en PPP de múltiples enlaces
 - Interposición del tráfico de voz entre paquetes de datos fragmentados en Frame Relay
 - Se pasa por alto la compresión y el cifrado de paquetes PPP o Frame Relay para el tráfico de voz
 - Dirección de bucle de retorno IP
Este soporte permite que los usuarios definan las direcciones IP en una interfaz especial para soportar la Pasarela TN3270, Network Dispatcher y los requisitos de IPSec.
 - IPv6
 - Se proporciona una función de direccionamiento interdominio (BGP4+) para IPv6 que soporta el direccionamiento IPv6 y la información de direcciones y utiliza TCP6 para el transporte.
 - El tráfico IPv6 se soporta a través de LAN Emulation de Ethernet ATM sin encapsulación ni túneles.
 - Múltiples vías de acceso de reenvío
El direccionamiento IP puede utilizar hasta cuatro rutas estáticas con igual coste para soportar múltiples enlaces paralelo para una dirección y máscara determinadas.
 - Agregación de ruta IP
 - Mejoras en multidifusión:
 - Protocol Independent Multicast-Dense Mode (PIM-DM) para IPv4.
 - Ahora, los administradores de la red pueden controlar el flujo de los datos de multidifusión IP de entrada y salida de las redes utilizando los filtros de tráfico de entrada y de salida.
 - Not-so-stubby area (NSSA)
OSPF soporta not-so-stubby area (NSSA) tal como se define en RFC 1587 y ahora se soporta el último borrador de Internet.

Resumen de los cambios

- Random Early Detection (RED)
- Mejoras en la política de servicios diferenciados
- Mejoras en VRRP:
 - La dirección MAC puede utilizarse en lugar de una dirección MAC virtual para identificar una pasarela redundante; esto puede ofrecer una mejora en el rendimiento.
 - Cuando hay más de un candidato de reserva disponible, se pueden configurar opciones de preferencia.
 - Para seleccionar el direccionador IP maestro, pueden utilizarse criterios adicionales como, por ejemplo, una ruta disponible o una interfaz de red, para soportar funciones que no son IP.
- Interfaz de marcación a petición alternativa para el redireccionamiento WAN
- Mejoras en TN3270
 - Superación de las LU
 - Equilibrio de la carga de la agrupación de LU
 - Desconexión Talk 5 de las sesiones TN3270
 - Información de informes adicionales
 - Soporte de las direcciones 1 y 255
- Mejoras en Network Dispatcher
 - Anuncio de las direcciones del grupo de asignadores de tareas de la red por protocolos de direccionamiento
 - Un nuevo asesor SSL
- Soporte de PU1 SDLC DLSw
- Soporte de la encapsulación Ethernet para la Ethernet de tipo II (valor por omisión) y 802.3 simultáneamente en la misma interfaz
- Mejoras en DHCP:
 - Copia de seguridad del disco fijo para información de alquiler
 - Soporte de múltiples direcciones IP para las interfaces DHCP
 - Soporte de alquiler corto
- Mejoras en RADIUS
 - Posibilidad de escalas de Radius
 - Inicio de sesión de Last Resort
- Posibilidad de escalas de L2TP
- Mejora en Thin Server
 - Conexión a un servidor maestro alternativo o de reserva
- Mejoras en la recuperación de archivos de servicios

Aclaraciones y correcciones

En las copias impresas y PDF, los cambios técnicos y las adiciones se indican por una línea vertical (|) situada a la izquierda del cambio.

Network Utility

Network Utility es un producto que consta de varios modelos del 2216. Proporciona varios subconjuntos de funciones del 2216, tal como se muestra en Tabla 1 en la página xxxvii.

Funciones de software soportadas por Network Utility

Cada modelo de Network Utility proporciona un subconjunto de las funciones de software del 2216, tal como se muestra en la Tabla 1. La Antememoria del servidor de la web (WSC) del 2216 Modelo 400 da soporte a protocolos IP y no proporciona funciones de APPN.

Tabla 1. Funciones de código soportadas en el 2216 Modelo 400 y en Network Utility

Función o protocolo	Disponible para el 2216 Modelo 400 Base	Disponible para la WSC del 2216 Modelo 400	Disponible para Network Utility Modelo TN1	Disponible para Network Utility Modelo TX1
TN3720E	Sí ¹	—	Sí ¹	—
Antememoria de IBM eNetwork Host on-Demand Client para TN3720E	Sí ¹	—	Sí ¹	—
Definición de LU dinámica iniciada por sistema principal para TN3720E	Sí ¹	—	Sí ¹	—
Múltiples SA de PU sobre DLSw para TN3720E	Sí ¹	—	Sí ¹	—
Network Dispatcher	Sí	Sí	Sí	Sí
Server Advisor (o Network Dispatcher Advisor) para TN3720E	Sí	Sí ²	Sí	Sí ²
Reserva de ancho de banda y puesta en cola según prioridad	Sí	Sí	Sí	Sí
Fragmentación de paquetes de Frame Relay	Sí	Sí	Sí	Sí
Reenvío de paquetes de Voz a través de Frame Relay	Sí	Sí	Sí	Sí
Filtro del MAC	Sí	Sí	Sí	Sí
Restauración de WAN	Sí	Sí	—	—
Redireccionamiento de WAN	Sí	Sí	—	—
Compresión de datos	Sí	Sí	Sí	Sí
Subsistema de codificación	Sí	Sí	Sí	Sí
Cifrado	Sí	Sí	Sí	Sí
Conmutación del enlace de datos (DLSw)	Sí	—	Sí	Sí
Calidad de los servicios (QoS)	Sí	Sí	Sí	Sí
IPSec (Seguridad de IP)	Sí	Sí	Sí	Sí
Servicios diferenciados	Sí	Sí	Sí	Sí
L2TP	Sí	Sí	Sí	Sí
L2F	Sí	Sí	Sí	Sí
PPTP	Sí	Sí	—	—

Resumen de los cambios

Tabla 1. Funciones de código soportadas en el 2216 Modelo 400 y en Network Utility (continuación)

Función o protocolo	Disponible para el 2216 Modelo 400 Base	Disponible para la WSC del 2216 Modelo 400	Disponible para Network Utility Modelo TN1	Disponible para Network Utility Modelo TX1
Conversión de direcciones de red	Sí	Sí	Sí	Sí
AAA (Seguridad de la autenticación, autorización y contabilidad)	Sí	Sí	Sí	Sí
RSVP	Sí	Sí	Sí	Sí
Servicios de DHCP	Sí	Sí	Sí	Sí
Servicios de directorios: el soporte de LDAP	Sí	Sí	Sí	Sí
IPv6	Sí	—	Sí	Sí
Thin Server	Sí	—	—	—
Antememoria del servidor de la web	—	Sí	—	—
Sondeo de grupos primarios para SDLC	Sí	—	Sí	Sí
Comunicación simultánea en dos direcciones para SDLC	Sí	—	Sí	Sí
IPX	Sí	—	—	—
Appletalk	Sí	—	—	—
DECnet IV	Sí	—	—	—
OSI	Sí	—	—	—
Banyan Vines	Sí	—	—	—
DIALs	Sí	Sí	Sí ³	Sí ³
Funciones de APPN				
Branch Extender	Sí	—	Sí	Sí
Peticionario de LU dependientes (DLuR)	Sí	—	Sí	Sí
Enterprise Extender	Sí	—	Sí	Sí
Extended Border Node	Sí	—	Sí	Sí
Direccionamiento de alto rendimiento (HPR)	Sí	—	Sí	Sí
Nodo de red (NN)	Sí	—	Sí	Sí
<ol style="list-style-type: none"> 1. Ésta es una función cuyo precio va aparte 2. En la comunicación con un servidor TN3270E de un producto de direccionamiento de IBM 3. Sólo accesible si se utilizan las funciones de túnel. Las funciones de túnel incluyen L2TP, PPTP y L2F. 				

Parte 1. Comprensión y utilización del software

Capítulo 1. Introducción

Este capítulo le muestra cómo empezar a utilizar los siguientes componentes relacionados con el Conmutador IBM 2216 Modelo 400 (2216) y Multiprotocol Access Services:

- Terminales de consola de dispositivo
- Software de dispositivo (Multiprotocol Access Services)
- Interfaz del usuario del software de dispositivo

La información de este capítulo se divide en las secciones siguientes:

- “Antes de empezar”
- “Acceso al software mediante consolas locales y remotas”
- “Explicación del sistema de interfaces del usuario” en la página 6

Antes de empezar

Antes de empezar, consulte la siguiente lista de comprobación para verificar que el dispositivo esté instalado correctamente.

¿Ha...

- Instalado todo el hardware necesario?
- Conectado el terminal de consola (terminal de vídeo) al dispositivo?

Atención: Si está utilizado un terminal conectado a un puerto de servicio para configurar o supervisar el IBM 2216 y no se puede leer el terminal de servicio, necesita modificar algunos parámetros de la configuración.

Consulte la documentación del hardware.

- Conectado el dispositivo a la red utilizando las interfaces de red y los cables correctos?
- Ejecutado todos los diagnósticos de hardware necesarios?

Para obtener más información sobre alguno de estos procedimientos, consulte el manual *IBM 2216 Nways Multiaccess Connector Installation and Initial Configuration Guide*.

Migración al release actual

Consulte la publicación *2216 Nways Multiaccess Connector Service and Maintenance Manual* para obtener más información sobre la migración a un nuevo nivel de código.

Acceso al software mediante consolas locales y remotas

La consola de dispositivo le permite utilizar la interfaz de usuario del dispositivo para supervisar la función del software de red del dispositivo. El dispositivo soporta consolas locales y remotas.

Consolas locales

Las consolas locales se conectan directamente mediante un cable EIA 232 (RS-232) o mediante módems al dispositivo. Es posible que tenga que utilizar una consola local durante la instalación inicial del software. Después de la conexión de configuración inicial, puede conectarse utilizando Telnet, siempre que se haya

habilitado el reenvío IP. (Consulte la publicación *Consulta de configuración y supervisión de protocolos* para obtener más información sobre la habilitación del reenvío IP.)

Cuando se inicia por primera vez el dispositivo configurado, aparece un mensaje de arranque en la pantalla, seguido del indicador OPerator CONsole u OPCON (*). El indicador * indica que el dispositivo está preparado para aceptar mandatos OPCON.

Tendrá que utilizar un terminal ASCII conectado al puerto de servicio del 2216 para configurarlo inicialmente.

Importante: La basura, los caracteres aleatorios, los signos de interrogación o la imposibilidad de conectar el terminal al puerto de servicio del 2216 pueden tener muchas causas. La lista siguiente contiene algunas de ellas:

- La causa más común de basura o de caracteres aleatorios en la consola de servicio es que la velocidad en baudios no está sincronizada con el IBM 2216.

Si el 2216 está establecido en una velocidad en baudios específica, el terminal o emulador de terminal debe establecerse en la misma velocidad en baudios.

Si el IBM 2216 está establecido en baudios automáticos (es el valor por omisión), pulse la secuencia de teclas de interrupción del terminal y pulse **Intro**.

La secuencia de teclas de interrupción típica para emuladores de terminal PC es Alt-B (consulte la documentación del emulador de terminal). La mayoría de terminales ASCII tienen la tecla **Inter** (que a menudo se utiliza con la tecla **Control**).

Consulte la documentación del hardware para obtener más información.

- Tomas de tierra (ca) defectuosas del terminal o dispositivo.
- Cable EIA 232 (RS-232) defectuoso, blindado incorrectamente o con una toma de tierra incorrecta entre el terminal y el IBM 2216.
- Terminal o emulador de terminal defectuoso.
- Placa del sistema del IBM 2216 defectuosa.
- Altos niveles de interferencias electromagnéticas (EMI) en el ambiente.
- Perturbaciones de la línea de alimentación.

Tras configurar inicialmente el 2216, no necesitará una consola local para el funcionamiento del dispositivo, siempre que haya habilitado IP.

El software de dispositivo maneja automáticamente la actividad de la consola. Cuando actualice el software, puede que necesite utilizar la consola local. Para obtener información sobre la conexión y configuración de las consolas locales, consulte la publicación *IBM 2216 Nways Multiaccess Connector Installation and Initial Configuration Guide*.

Consolas remotas

Las consolas remotas se conectan al dispositivo utilizando un protocolo de terminal remoto estándar. Las consolas remotas proporcionan la misma función que las consolas locales, excepto en que debe utilizarse una consola local para la

configuración inicial. No puede utilizar más de dos consolas remotas a la vez en un dispositivo. Puede conectar consolas remotas al dispositivo mediante una conexión Telnet. Tiene la opción de inhabilitar esta característica.

Conexiones Telnet

El dispositivo soporta el cliente y el servidor Telnet. La consola remota del dispositivo actúa como servidor Telnet. El dispositivo actúa como cliente Telnet cuando se establece la conexión desde el dispositivo con otro dispositivo o con un sistema principal que utiliza el mandato **telnet** en el proceso OPCON (*).

Nombres y contraseñas de inicio de sesión remoto

Durante un inicio de sesión remoto, el dispositivo le solicita el nombre de inicio de sesión y la contraseña. Puede visualizar el nombre de inicio de sesión cuando ha iniciado la sesión en el dispositivo desde una consola remota utilizando un mandato **status** de dispositivo.

Inicio de sesión remota o localmente

El inicio de sesión en una consola local es igual que el inicio de sesión en una consola remota excepto en que debe conectarse al dispositivo iniciando Telnet en el sistema principal. Para iniciar la sesión remotamente, empiece por el paso 1. Para iniciar la sesión localmente, empiece por el paso 3.

Para iniciar la sesión desde una consola remota:

1. Conéctese al dispositivo iniciando Telnet en el sistema principal. El sistema principal es aquél al que se conectan los terminales remotos.
2. Proporcione el nombre del dispositivo o la dirección de Internet Protocol (IP).
Para utilizar nombres de dispositivo, la red debe tener un servidor de nombres. Emita el nombre del dispositivo o la dirección IP, tal como se muestra en el ejemplo siguiente:

```
% telnet brandenburg
```

```
o
```

```
% telnet 128.185.132.43
```

Llegado a este punto, no hay ninguna diferencia entre haber iniciado la sesión remota o localmente.

3. Si se le solicita, entre el nombre de inicio de sesión y la contraseña.

```
login:  
Password:
```

Es posible que haya un inicio de sesión y ninguna contraseña. La contraseña controla el acceso al dispositivo. Si no se ha establecido ninguna contraseña, pulse la tecla **Intro** en el indicador Password:. Los inicios de sesión no se establecen automáticamente. Por razones de seguridad, puede configurar nombres de usuario y contraseñas utilizando el mandato **add user** en el proceso CONFIG. Para obtener información adicional, consulte la descripción del mandato **add user** en 83. Recuerde que debe volver a cargar para activar los cambios.

Nota: Si no entra ningún nombre de inicio de sesión y una contraseña válida durante el primer minuto después del indicador inicial, o si entra una contraseña incorrecta tres veces sucesivas, el dispositivo desactiva la conexión Telnet.

4. Pulse la tecla **Intro** para visualizar el indicador de asterisco (*).

Es posible que tenga que pulsar la tecla **Intro** más de una vez o que tenga que pulsar **Control-P** para obtener el indicador *.

Cuando esté en este nivel, puede empezar a entrar mandatos desde el teclado. Pulse la tecla **Retroceso** para suprimir el último carácter escrito en la línea de mandatos. Pulse la tecla **Supr** o las teclas **Control-U** para suprimir toda la entrada de la línea de mandatos y volver a entrar un mandato. Consulte las secciones “Finalización del mandato” en la página 23 y “Histórico de mandatos” en la página 27 para obtener más información.

También puede utilizar los mandatos locales Telnet en el cliente Telnet para cerrar la conexión Telnet.

Nota: Si utiliza un terminal VT100, no pulse la tecla **Retroceso**, porque inserta caracteres invisibles. Utilice la tecla **Supr**.

5. Salga del dispositivo tal como se describe en la sección “Salir del dispositivo”.

Volver a cargar el dispositivo

Utilice el mandato **reload** para rearrancar el dispositivo mediante la carga de una nueva copia de la configuración desde la memoria. Siempre que cambie un parámetro configurable por el usuario que no sea configurable dinámicamente, debe volver a cargar el dispositivo para que el cambio surta efecto. Por ejemplo:

```
* reload
```

```
The configuration has been changed, save it? (Yes or [No] or Abort)
```

```
Are you sure you want to reload the gateway? (Yes or [No]): yes
```

Salir del dispositivo

Vuelva al indicador * y utilice el mandato **logout** para cerrar la conexión Telnet. Por ejemplo:

```
IP Config> exit
Config> Control-P
* logout

%
```

También puede utilizar los mandatos locales Telnet en el cliente Telnet para cerrar la conexión Telnet.

Explicación del sistema de interfaces del usuario

El software es un sistema multitarea que planifica la utilización de la CPU entre varios procesos y dispositivos de hardware. El software de dispositivo:

- Proporciona la gestión del tiempo y de la memoria y soporta las consolas de operador locales y remotas desde las cuales puede ver y modificar los parámetros operativos del dispositivo.
- Consta de módulos funcionales que incluyen varios procesos de interfaz de usuario, todos los controladores de interfaz de red y todos los reenviadores de protocolo adquiridos con el dispositivo.

Comprensión de la interfaz de usuario de primer nivel

La interfaz de usuario para el software consta del menú principal (proceso) y de varios menús subsidiarios (procesos). Estos menús están relacionados con los distintos niveles de procesos del software.

El primer nivel de procesos consta de los procesos OPCON y CONFIG-ONLY. En la mayoría de casos, utilizará el proceso OPCON para acceder al segundo nivel para configurar o utilizar los servicios básicos, las características, las interfaces y los protocolos que va a ejecutar en el IBM 2216.

El segundo nivel contiene procesos como, por ejemplo, Configuración (CONFIG), Consola (GWCON) y Sistema de anotación cronológica de sucesos (MONITR). Puede utilizar los mandatos OPCON **configuration**, **console** o **event** para acceder a estos procesos de segundo nivel. Alternativamente, puede utilizar el mandato **status** para listar los procesos de segundo nivel y, después, utilizar el mandato **talk pid** para acceder a los procesos de segundo nivel. Hay procesos que no se pueden utilizar en el software. Consulte en la Tabla 2 en la página 10 una visión general de los procesos.

La Figura 1 muestra los procesos y la forma en en que están organizados en la estructura del software de dispositivo.

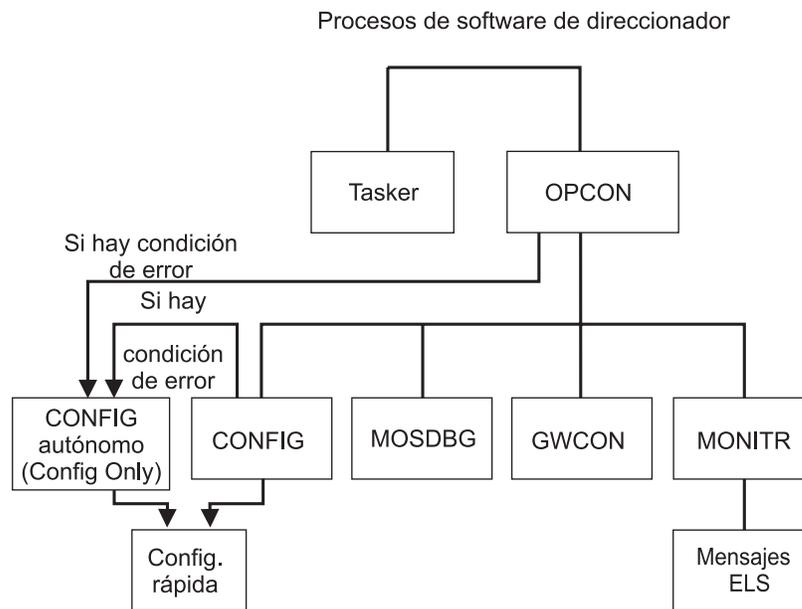


Figura 1. Multiprotocol Access Services

La Figura 2 en la página 8 es un ejemplo de la relación entre los distintos niveles de procesos.

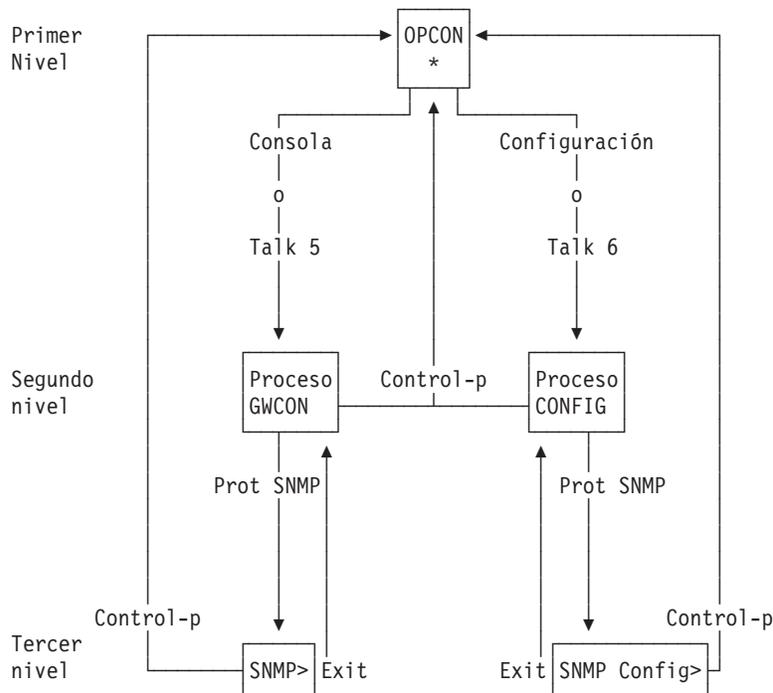


Figura 2. Relación de los procesos y mandatos

Nota: En la Figura 2 también aparecen los diversos mandatos para acceder a cada nivel de proceso y volver de los mismos,

Consulte la sección “¿Qué es el proceso OPCON?” en la página 33 para obtener más información acerca de OPCON y “Modalidad de Sólo configuración” en la página 67 para obtener más información acerca de CONFIG-ONLY.

El proceso ROPCON maneja el proceso desde consolas remotas y es esencialmente igual al proceso OPCON.

Proceso de configuración rápida

La configuración rápida o Quick Config, le permite configurar rápidamente las partes del dispositivo sin tener que utilizar mandatos específicos del sistema operativo. Cuando se carga inicialmente, se reinicia o se vuelve a cargar el dispositivo sin ninguna configuración, se entra en Sólo configuración y se puede acceder a los menús de la Configuración rápida desde ese proceso. Si el dispositivo tiene dispositivos configurados y estos no tienen ningún protocolo configurado, el dispositivo inicia automáticamente Sólo configuración y, después, entra en la Configuración rápida.

También puede entrar en la Configuración rápida desde el proceso CONFIG utilizando el mandato **qconfig**.

Seguridad del sistema

Se pueden añadir múltiples usuarios con permisos de inicio de sesión utilizando el mandato **add user**. Consulte la sección “Configuración del acceso de usuario” en la página 70 para ver los detalles sobre la seguridad y para obtener información sobre los mandatos **set password** y **add user**.

Capítulo 2. Utilización del software

Este capítulo describe cómo utilizar el software. Consta de:

- “Entrada de mandatos”
- “Conexión a un proceso”
- “Algunas sugerencias sobre la configuración” en la página 11
- “Acceso a los procesos de segundo nivel” en la página 14
- “Acceso a los procesos de tercer nivel” en la página 16
- “Finalización del mandato” en la página 23
- “Histórico de mandatos” en la página 27

Entrada de mandatos

Al escribir un mandato, recuerde lo siguiente:

- Puede escribir solamente las letras necesarias del mandato para que sea exclusivo entre los mandatos disponibles. Por ejemplo, para ejecutar el mandato **reload** debe entrar **rel** como mínimo. El número mínimo de caracteres necesarios se subraya en los capítulos de sintaxis de mandatos.
- Los mandatos no son sensibles a las mayúsculas y minúsculas.
- A veces, sólo es necesaria la primera letra del mandato (y las opciones subsiguientes) para ejecutar el mandato. Por ejemplo, si se escribe **s** en el indicador ***** y después se pulsa la tecla **Intro** provoca la ejecución del mandato **status**.
- Cuando está habilitada la finalización de mandatos, puede pulsar **Esc** y entrar **?** para obtener ayuda acerca de la entrada de mandatos. Consulte las secciones “Finalización del mandato” en la página 23 y “Histórico de mandatos” en la página 27 para obtener más información.

Conexión a un proceso

Cuando se inicia el dispositivo, la consola visualiza un mensaje de arranque. El indicador **OPCON (*)** aparece en la pantalla indicando que está en el proceso **OPCON** y que puede empezar a entrar mandatos **OPCON**. Este es el indicador de mandatos desde el cual se comunica con los diferentes procesos.

Los mandatos que se necesitan con más frecuencia aparecen antes del separador “- - - -”. Entre el mandato adecuado en el indicador **OPCON (*)**. Consulte la Tabla 4 en la página 34 para ver una lista de mandatos.

Alternativamente, puede:

1. Averiguar el número de ID del proceso (PID) entrando el mandato **status** en el indicador *****.

El mandato **status** visualiza información acerca de los procesos de dispositivo como, por ejemplo, los ID de proceso (PID), los nombres de proceso y el estado del proceso. La emisión del mandato **status** aparece en el ejemplo siguiente:

```
* status
Pid  Name   Status TTY  Comments
1    COpCn1 RDY   TTY0
2    Monitr DET   --
3    Tasker RDY   --
4    MOSDBG DET   --
5    CGWCon DET   --
```

```

6 Config DET --
7 ELScn DET --
8 ROpCn1 IDL TTY1 128.185.210.125
9 ROpCn2 IDL TTY2

```

- Utilice el mandato **talk pid**, donde *pid* es el número del proceso al que se desea conectar. (Para obtener más información acerca de estos y de otros mandatos OPCON, consulte la sección “¿Qué es el proceso OPCON?” en la página 33.)

Nota: No todos los procesos listados tienen una interfaz de usuario (por ejemplo, el proceso **talk 3**). El mandato **talk 4** es para que lo utilice el servicio técnico.

Identificación de los indicadores

Cada proceso utiliza un indicador diferente. Puede saber a qué proceso está conectada la consola por el indicador. (Si el indicador no aparece cuando entra el mandato **talk pid**, pulse **Intro** de nuevo.)

La lista siguiente muestra los indicadores para los cinco procesos principales:

Tabla 2. Procesos, su finalidad y mandatos para acceder a ellos

Proceso	Nivel y finalidad	Mandato para acceder	Indicador de entrada
OPCON	Nivel 1 - acceso a todos los niveles secundarios	Control-P	asterisco (*)
CONFIG	Nivel 2 - configuración de los servicios básicos y acceso al tercer nivel de configuración	Configuración o talk 6	Config >
GWCON	Nivel 2 - operación y supervisión de los servicios básicos y acceso a las operaciones y supervisión del tercer nivel	Consola o talk 5	signo más (+)
MONITR	Nivel 2 - visualización de mensajes	Suceso o talk 2	(ninguno)
ELScn	Nivel 2 - supervisión directa y acceso a la consola ELS	els o talk 7	ELS Secondary Console>
MOSDBG	Nivel 2 - entorno de diagnósticos	talk 4	db>
DIAGS	Nivel 2 - ejecución de diagnósticos de hardware	diags	
Nota: Únicamente entre el mandato talk 4 bajo instrucción del servicio técnico.			

En el nivel de indicador OPCON, puede empezar a entrar mandatos desde el teclado. Utilice la tecla **Retroceso** para suprimir el último carácter que ha escrito en la línea de mandatos. Utilice **Control-U** para suprimir toda la entrada de la línea de mandatos y volver a entrar un mandato. Consulte las secciones “Finalización del mandato” en la página 23 y “Histórico de mandatos” en la página 27 para obtener detalles adicionales o pulse **Escape** ?.

Cómo obtener ayuda

En los indicadores de mandatos, puede obtener ayuda en forma de listado de los mandatos disponibles del nivel actual. Para ello, escriba ? (el mandato **help**) y luego pulse **Intro**. Utilice ? para listar los mandatos disponibles que hay en el nivel

actual. Normalmente, puede entrar el signo ? después de un nombre de mandato específico si desea listar las opciones del mismo.

Cómo salir de un entorno de nivel inferior

La naturaleza de múltiples niveles del software le coloca en entornos de nivel secundario, terciario e incluso inferiores al configurar el 2216 o al servirse del mismo. Para volver al nivel superior más próximo, entre el mandato **exit**. Para obtener el nivel secundario, continúe entrando **exit** hasta que reciba el indicador de nivel secundario (Config> o +).

Por ejemplo, para salir del proceso de configuración de protocolos de ASRT:

```
ASRT config> exit
Config>
```

Si tiene que obtener el nivel primario (OPCON), entre el carácter de interceptación (**Control-P** por omisión).

Volver a OPCON

Para volver al indicador OPCON (*), pulse **Control-P**. Siempre debe volver a OPCON antes de poder comunicarse con otro proceso. Por ejemplo, si está conectado al proceso de consola (GWCON) y desea conectarse al proceso CONFIG, debe pulsar **Control-P** para volver primero a OPCON. La combinación de teclas **Control-P** es el *carácter de interceptación* por omisión.

Si utiliza el carácter de interceptación desde un menú del tercer nivel o inferior para volver al indicador *, la próxima vez que utilice el mandato **talk** para conectarse con el mismo proceso, volverá a entrar en un menú del mismo nivel. Este enlace desaparece cuando se reinicializa el dispositivo.

Algunas sugerencias sobre la configuración

La configuración del 2216 es diferente dependiendo de si lo configura por primera vez, si crea una configuración basada en otra existente o si sólo actualiza una configuración. Utilice las secciones siguientes como guía para averiguar el mejor procedimiento que puede utilizar, dependiendo de las necesidades.

Creación de una primera configuración

Este procedimiento supone que no tiene ningún otro 2216 que contenga una configuración similar a la que está configurando para el 2216. El procedimiento supone también que acaba de desembalar el 2216. Aunque este procedimiento especifica un orden, puede efectuar la configuración real (después del paso 3) en cualquier orden.

Para configurar el IBM 2216 por primera vez:

1. Examine el 2216 que está configurando para determinar qué interfaces tiene que configurar. Anótelas para utilizarlas luego.
2. Conéctese al 2216, tal como se describe en la sección "Acceso al software mediante consolas locales y remotas" en la página 3.
3. Inicialmente, configure un puerto en el 2216 y, como mínimo, una dirección IP interna para el dispositivo mediante la Configuración rápida, tal como se describe en la sección "Configuración rápida" en la página 69 o en el "Apéndice A. Consulta para la configuración rápida" en la página 809. Configure lo mínimo necesario para permitirle establecer una conexión Telnet con el dispositivo.

4. Configure cualquier servicio básico como, por ejemplo, las opciones de arranque. Acceda al proceso de configuración descrito en la sección “Acceso al proceso de configuración, CONFIG (Talk 6)” en la página 14.
5. Configure las interfaces. Acceda al proceso de configuración de interfaces, tal como se describe en la sección “Acceso al proceso de configuración de interfaces de red” en la página 16.
6. Configure cualquier característica necesaria. Acceda al proceso de configuración de la característica, tal como se describe en la sección “Acceso a los procesos de configuración y operación de características” en la página 21.
7. Configure cualquier protocolo que se ejecutará en este dispositivo. Acceda al proceso de configuración de protocolos, tal como se describe en la sección “Acceso a los procesos de configuración y operación de protocolos” en la página 22.

Nota: En este paso, configurará como mínimo IP.

8. Vuelva a cargar el dispositivo tal como se describe en la sección “Volver a cargar el dispositivo” en la página 6.

Basar una configuración en una configuración existente

Esta sección describe cómo:

- Basar una configuración en la configuración de un 2216 en funcionamiento
- Actualizar de manera permanente la configuración de un 2216
- Actualizar temporalmente la configuración de un 2216 mientras el 2216 está en funcionamiento

Configuración existente como base

Si ya tiene un 2216 que tiene las mismas interfaces, características y protocolos que desea configurar en un nuevo 2216, puede ahorrar tiempo basando la configuración en el 2216 existente. Puede realizar este tipo de configuración utilizando la interfaz de línea de mandatos o utilizando el programa de configuración que se suministra con el 2216. En ambos casos, los procedimientos suponen que el 2216 no está en la red de producción.

Para basar una configuración en una ya existente utilizando la interfaz de línea de mandatos:

1. Obtenga una copia de la configuración que desea utilizar.
 - a. Entre **talk 6** en el indicador OPCON (*).
 - b. Entre **boot** en el indicador Config>.
 - c. Entre el mandato **copy configuration archivo** en el indicador Boot config>. Consulte la sección “Capítulo 5. Utilización de BOOT Config para efectuar la gestión de cambios” en la página 47 para obtener más información.
2. Conéctese al 2216 que está configurando.
3. Cargue la configuración que ha obtenido en el paso 1 en el 2216 utilizando TFTP GET. Consulte la sección “Capítulo 5. Utilización de BOOT Config para efectuar la gestión de cambios” en la página 47.
4. Actualice la configuración.
5. Grabe la configuración. Consulte la sección “¿Qué es CONFIG?” en la página 67.
6. Vuelva a cargar el 2216.

Para basar una configuración en una ya existente utilizando el programa de configuración:

1. Inicie el programa de configuración.
2. Recupere la configuración del 2216 en la que desea basar la nueva configuración.
3. Realice los cambios necesarios para la nueva configuración. Estos cambios incluyen las direcciones, los nombres de sistemas principales, los usuarios y otros elementos.
4. Guarde la configuración con un nombre diferente del que ha utilizado para recuperar la configuración.
5. Envíe la configuración al 2216 que está configurando.
6. Vuelva a cargar el 2216.

Para ver los detalles sobre la utilización del programa de configuración, consulte la publicación *Guía del usuario del Programa de Configuración para productos Nways Multiprotocol y Access Services*.

Actualización permanente de una configuración

Para actualizar permanentemente una configuración:

1. Acceda al 2216 que está actualizando, tal como se describe en la sección “Acceso al software mediante consolas locales y remotas” en la página 3. Verá el indicador *.
2. Entre el mandato **talk 6** para acceder al proceso de configuración.
3. Entre los mandatos adecuados para acceder al proceso del tercer nivel que configura las áreas que está modificando.
4. Entre **exit** tantas veces como sea necesario para volver al proceso de configuración.
5. Grabe la configuración. Consulte la sección “¿Qué es CONFIG?” en la página 67.
6. Vuelva a cargar el 2216.

Actualización temporal de una configuración

La posibilidad de actualizar temporalmente una configuración le permite realizar cambios en algunas características operativas de un 2216 hasta que pueda realizar las actualizaciones permanentes en la configuración. Esto le permite implementar los cambios inmediatamente para resolver problemas o mejorar el rendimiento y evitar una interrupción durante las horas punta. después, puede hacer que los cambios en la configuración sean permanentes y planificar una interrupción para que pueda volver a cargar para recoger el cambio.

Para actualizar temporalmente una configuración:

1. Acceda al 2216 que está actualizando, tal como se describe en la sección “Acceso al software mediante consolas locales y remotas” en la página 3. Verá el indicador *.
2. Entre el mandato **talk 5** para acceder al proceso de operación/supervisión.

Nota: No todos los tipos de interfaz, protocolo o característica permiten realizar cambios en la configuración mediante el mandato talk 5.

3. Entre los mandatos adecuados para acceder al proceso del tercer nivel que supervisa las áreas que está modificando.
4. Entre **exit** tantas veces como sea necesario para volver al proceso de operación/supervisión.
5. Entre **Control-P** para volver al indicador *.

6. Salga del dispositivo, tal como se describe en la sección “Salir del dispositivo” en la página 6.

Acceso a los procesos de segundo nivel

Todas las interfaces, las características y los protocolos tienen mandatos que se utilizan para acceder a los procesos siguientes:

- El proceso de configuración para configurar inicialmente y habilitar la interfaz, la característica o el protocolo, así como para realizar cambios posteriores en la configuración.
- El proceso de operación/supervisión para visualizar información acerca de todas las interfaces, características o protocolos, para realizar cambios temporales en la configuración o para activar los cambios en la configuración.

También puede configurar o utilizar algunos servicios básicos del sistema mediante los procesos de segundo nivel. La descripción de los mandatos que realizan estas funciones empieza en la sección “¿Qué es CONFIG?” en la página 67.

Las secciones siguientes describen los procedimientos para acceder a los procesos de segundo nivel.

Acceso al proceso de configuración, CONFIG (Talk 6)

Se accede a cada proceso de configuración a través del proceso CONFIG del dispositivo. CONFIG es el proceso de segundo nivel de la interfaz del usuario del dispositivo que le permite comunicarse con los procesos del tercer nivel. Los procesos de protocolo son ejemplos de procesos del tercer nivel.

La interfaz de mandatos CONFIG está compuesta por niveles de menú. Las interfaces de mandatos de configuración de protocolo son menús de la interfaz CONFIG. Cada interfaz de configuración de protocolo tiene su propio indicador. Por ejemplo, el indicador para la interfaz de mandatos del protocolo SNMP es `SNMP config>`.

Las secciones siguientes describen estos procedimientos con más detalle.

Entrada en el proceso CONFIG

Para entrar en el proceso CONFIG desde OPCON y obtener el indicador CONFIG, entre el mandato **configuration**. Alternativamente, puede entrar el mandato **talk** de OPCON y el PID para CONFIG. El PID para CONFIG es 6.

* **configuration**

0

* **talk 6**

Se visualiza el indicador CONFIG (`Config>`) en la consola. Si no aparece el indicador, pulse la tecla **Intro** de nuevo.

Proceso de configuración rápida: La configuración rápida o Quick Config, le permite configurar rápidamente las partes del dispositivo sin tener que utilizar mandatos específicos del sistema operativo. Se entra en los menús de la Configuración rápida desde el proceso CONFIG utilizando el mandato **qconfig** (consulte la sección “Configuración rápida” en la página 69).

Volver a cargar el dispositivo

Los cambios que realice en los parámetros de protocolo a través de CONFIG no surten efecto hasta que active la red que contiene los cambios dinámicos o vuelva a cargar el software del dispositivo.

Nota: Debe entrar el mandato **write** para guardar los cambios en la memoria instantánea del dispositivo.

Para volver a cargar el dispositivo, entre el mandato **reload** de OPCON. Por ejemplo:

```
* reload
Are you sure you want to reload the gateway? (Yes or No): yes
```

Acceso al proceso de operación/supervisión de la consola, GWCON (Talk 5)

Para ver la información acerca de las interfaces, las características o los protocolos o para cambiar los parámetros mientras está en ejecución, debe acceder y utilizar el proceso de operación (supervisión). Las interfaces de mandatos operativos son modalidades de la interfaz GWCON. En la modalidad GWCON, cada interfaz, característica o interfaz de protocolo tiene su propio indicador. Por ejemplo, el indicador para el protocolo SNMP es `SNMP>`.

Nota: Cualquier parámetro que cambie en este proceso no permanecerá activo si se produce algún suceso que haga que el 2216 vuelva a cargar el código operativo como, por ejemplo, un corte en el suministro eléctrico o la entrada del mandato **reload**.

Las secciones siguientes describen estos procedimientos con más detalle.

Entrada en el proceso de mandatos GWCON

Para entrar en el proceso GWCON desde OPCON y obtener el indicador GWCON, entre el mandato **console**. Alternativamente, puede entrar el mandato **talk** y el PID para GWCON. El PID para GWCON es 5. Por ejemplo:

```
* console

O
* talk 5
```

Entonces, se visualiza el indicador GWCON (+) en la consola. Si no aparece el indicador, pulse **Intro** de nuevo.

Acceso al proceso de consola ELS secundario, ELSCON (Talk 7)

La consola ELS secundaria proporciona un acceso conveniente al ELS `talk 5` de GWCON sin interrumpir el estado actual de GWCON. Puede que esté ejecutando **ping** en `talk 5` o en una estructura de menú `talk 5` y desee controlar ELS sin interrumpir el estado actual de GWCON. La consola ELS secundaria (Talk 7) sirve para este fin.

Para entrar en el proceso de Consola ELS secundaria (ELSCON) desde OPCON y obtener el indicador de Consola ELS secundaria, entre el mandato **els**. Alternativamente, puede entrar el mandato **talk 7**.

En el ejemplo siguiente, se visualiza otro suceso ELS mientras se ejecuta un mandato **ping**.

Nota: Se utiliza el carácter de interceptación (Control-P por omisión) para obtener el indicador OPCON (*).

```
*talk 5
+protocol ip
IP>ping 10.0.0.9
PING 10.0.0.2 -> 10.0.0.9: 56 data bytes, ttl=64, every 1 sec.
```

```
*talk 7
```

```
ELS Secondary Console>display event ip.7
Complete
ELS Secondary Console>
*talk 2
00:20:48 IP.007: 10.0.0.2 -> 10.0.0.9
00:20:49 IP.007: 10.0.0.2 -> 10.0.0.9
```

Acceso a los procesos de tercer nivel

Después de acceder al segundo nivel, debe entrar mandatos en el tercer nivel para configurar o utilizar las interfaces, las características y los protocolos del IBM 2216. Las secciones siguientes describen cómo acceder a los procesos de tercer nivel.

Adición de dispositivos

Esta sección describe cómo utilizar el mandato **add device** para configurar las interfaces de red. Normalmente, una interfaz de red es un adaptador, pero también puede ser una definición utilizada por un proceso operativo. Por ejemplo, se pueden asignar dos direcciones IP a un puerto y considerar cada una como una interfaz. Después de establecer una interfaz utilizando el mandato **add device**, puede acceder a los procesos de configuración y operación de la interfaz de red, por ejemplo, los procesos de supervisión Talk 5. Estos procesos se utilizan para cambiar y supervisar los parámetros configurables por el software para las interfaces de red que se utilizan en el dispositivo.

Acceso al proceso de configuración de interfaces de red

Utilice el procedimiento siguiente para acceder al proceso de configuración del dispositivo. Este proceso proporciona acceso al proceso de *configuración* de una interfaz específica.

1. En el indicador OPCON, entre el mandato **configuration**.

```
* configuration
```

Después de entrar el mandato **configuration**, se visualiza el indicador CONFIG (Config>) en la consola. Si no aparece el indicador cuando entre **configuration**, pulse **Intro** de nuevo.

Utilice el mandato **add device** para crear una interfaz de red. El mandato **add device** asigna automáticamente el número de interfaz. (Entre **add device ?** para obtener una lista de tipos de dispositivo soportados.)

Estos son los tipos de dispositivos soportados:

- a. Adaptadores multipuerto

Cuando se especifica un nombre de dispositivo adaptador multipuerto con el mandato **add device**, se solicita el número de ranura del adaptador y el número de puerto del adaptador que desea utilizar para la interfaz.

Si desea utilizar varios puertos de un adaptador, debe entrar el mandato **add device** varias veces y especificar un número de puerto diferente cada vez.

Por ejemplo, entraría los siguientes mandatos para crear interfaces para los puertos 0 y 1 en el adaptador X.21 de 8 puertos de la ranura 7.

```
Config> add device x21
Device Slot #(1-8) [1]? 7
Device Port #(0-7) [0]? 0
Defaulting Data-link protocol to PPP
Adding X.21 PPP device in slot 7 port 0 as interface #6
Use "set data-link" command to change the data-link protocol
Use "net 6" to configure X.21 PPP parameters

Config> add device x21
Device Slot #(1-8) [1]? 7
Device Port #(0-7) [0]? 1
Defaulting Data-Link protocol to PPP
Adding X.21 PPP device in slot 7 port 1 as interface #7
Use "set data-link" command to change the data-link protocol
Use "net 7" to configure X.21 PPP parameters
```

Nota: Los números de puerto de adaptador serie se basan en 0. Los números de puerto para todos los demás adaptadores multipuerto se basan en 1.

Los adaptadores RDSI para 4 puertos en varios canales T1 y E1 le permiten configurar varios puertos con un mandato **add device**. Cuando se añade uno de estos adaptadores, el software le solicitará el rango de puertos que se ha de añadir. El ejemplo siguiente le muestra cómo se añadiría un adaptador RDSI para 4 puertos en varios canales T1 y E1 en la ranura 4 que está utilizando redes de marcación de entrada:

```
Device Slot #(1-8) [1]? 3
Device Port Range (1-8)
  Lowest Port #(1) [1]? 2
  Highest Port #(8) [8]? 2
Automatically add dial-in nets for this base net? (Yes or [No]): yes
Automatically enable IP for these dial-in nets?(Yes or [No]): yes
Enable as a Multilink PPP link?(Yes or [No]): yes
Adding 23 dial-in nets on top of base net 14
Adding 8-port ISDN Primary T1/J1 devices in slot 3 port 2 as interfaces #14.
Use "net 14" to configure 8-port ISDN Primary T1/J1 parameters.
```

b. Adaptadores de un solo puerto

Cuando se especifica un nombre de dispositivo adaptador de un solo puerto con el mandato **add device**, se solicita el número de ranura del adaptador.

El ejemplo siguiente añade una interfaz para el adaptador RDSI-PRI T1/J1 de un solo puerto en la ranura 2:

```
Config> add device t1-isdn
Device Slot #(1-8) [1]? 2
Adding ISDN Primary T1/J1 device in slot 2 port 1 as interface #7
Use "net 7" to configure ISDN Primary T1/J1 parameters
```

c. Circuitos de marcación

El ejemplo siguiente añade una interfaz de circuito de marcación:

```
Config> add device dial-circuit
Enter the number of PPP Dial Circuit interfaces [1]?
Adding device as interface 8
Base net for this circuit[0]?4
Defaulting Data-link protocol to PPP
Use "set data-link" command to change the data-link protocol
Use "net 8" command to configure circuit parameters
```

d. El ejemplo siguiente añade un circuito de marcación de entrada:

```
Config>add device dial-in
Enter the number of dial-in interfaces [1]?
Adding device as interface 5
Base net for this circuit [0]? 5
Defaulting Data-link protocol to PPP
Use "set data-link" command to change the data-link protocol
Use "net 5" command to configure circuit parameters
```

e. PPP de múltiples enlaces

El ejemplo siguiente añade una interfaz PPP de múltiples enlaces:

```
Config>add device multilink-ppp
Enter the number of Multilink PPP interfaces [1]?
Adding device as interface 7
Defaulting Data-link protocol to PPP
Use "net 7" command to configure circuit parameters
```

Notas:

- a. Cuando se crean interfaces para los adaptadores serie o circuitos de marcación, el tipo de enlace de datos por omisión es PPP. Sin embargo, puede utilizar el mandato **set data-link** para cambiar el tipo de enlace de datos. Consulte la Tabla 3 en la página 19 para ver los tipos de enlaces de datos soportados en puertos series y circuitos de marcación y la descripción del mandato **set data-link** en la página 106.
2. En el indicador Config>, entre el mandato **list devices** para visualizar los números de interfaz de red para los que el dispositivo está configurado actualmente, de la manera siguiente:

```
Config> list devices

Ifc 0 Token Ring           Slot: 1 Port: 1
Ifc 1 Token Ring           Slot: 1 Port: 2
Ifc 2 Token Ring           Slot: 2 Port: 1
Ifc 3 Token Ring           Slot: 2 Port: 2
Ifc 4 Ethernet             Slot: 4 Port: 1
Ifc 5 Ethernet             Slot: 4 Port: 2
Ifc 6 Ethernet             Slot: 5 Port: 1
Ifc 7 Ethernet             Slot: 5 Port: 2
Ifc 8 Ethernet             Slot: 6 Port: 1
Ifc 9 Ethernet             Slot: 6 Port: 2
Ifc 10 V.35/V.36 Frame Relay Slot: 8 Port: 0
Ifc 11 V.35/V.36 X.25      Slot: 8 Port: 1
Ifc 12 V.35/V.36 PPP       Slot: 8 Port: 2
Ifc 13 V.35/V.36 PPP       Slot: 8 Port: 3
Ifc 14 V.35/V.36 PPP       Slot: 8 Port: 4
Ifc 15 V.35/V.36 PPP       Slot: 8 Port: 5
```

3. Anote los números de interfaz.
4. Entre el mandato **network** de CONFIG y el número de la interfaz que desea configurar. Por ejemplo:

```
Config> network 1
```

Ahora, se visualiza el indicador de configuración adecuado (por ejemplo, TKR Config> para red en anillo), en la consola.

Nota: El usuario no puede configurar todas las interfaces de red. Para las interfaces que no se pueden configurar, se recibe el mensaje:

```
That network is not configurable
```

Restricciones del soporte del dispositivo IBM 2216: Se aplican las normas siguientes cuando se añaden dispositivos al IBM 2216:

- Pueden definirse un máximo de dos interfaces ATM.
- Pueden definirse un máximo de ocho interfaces RDSI-PRI con las restricciones siguientes:
 - No se pueden utilizar más de cuatro adaptadores de 1 puerto
 - No se puede utilizar más de un adaptador RDSI para 4 puertos en varios canales T1 y E1
- La adición de un dispositivo LAN en las ranuras 3, 4, 7 ó 8 inhabilitará la otra ranura del par. Por ejemplo, si añade un dispositivo LAN en la ranura 4, se inhabilitará la ranura 3. De igual modo, si añade un dispositivo en la ranura 3, se inhabilitará la ranura 4. Se aplican las mismas normas cuando se añade un dispositivo LAN en las ranuras 7 y 8.

- Todas las interfaces de un adaptador V.35/V.36 deben utilizar cables V.35 o cables V.36. El tipo de cable ramificado conectado al adaptador V.35/V.36 determina el tipo de cables (V.35 ó V.36) que puede utilizarse.

Visualización de la configuración de la interfaz: En los mismos indicadores de configuración de interfaz, puede listar la información de configuración específica de la interfaz seleccionada utilizando el mandato **list**. Por ejemplo:

```
TKR Config> list
Token-Ring configuration:
PACKET SIZE (INFO FIELD): 4472
Speed:                    16 Mb/sec
Media:                    Shielded
RIF Aging Timer:         120      Source Routing:      Enabled
MAC Address:             000000000000
```

Configuración de la interfaz de red: Consulte los capítulos específicos de esta guía para obtener información completa sobre la configuración de las interfaces de red del IBM 2216.

La Tabla 3 lista las arquitecturas de red y las interfaces soportadas para cada arquitectura.

Tabla 3. Arquitectura de red e interfaces soportadas

Arquitectura de red	Interfaces soportadas
ATM	MMF ATM de 155 Mbps de 1 puerto SMF ATM de 155 Mbps de 1 puerto
Red en Anillo 802.5	Red en Anillo de 2 puertos
Ethernet	<ul style="list-style-type: none"> • Ethernet de 10/100 Mbps de 1 puerto • Ethernet de 10 Mbps de 2 puertos
RDSI	<ul style="list-style-type: none"> • RDSI-PRI (T1/J1) de 1 puerto * • RDSI-PRI (E1) de 1 puerto * • RDSI para 4 puertos en varios canales T1 y E1 * <p>Nota: Las interfaces señaladas con un asterisco (*) se pueden utilizar como interfaces RDSI o canalizada.</p>
Punto a punto	Interfaces V.24/EIA 232E de 8 puertos, V.35/V.36 de 6 puertos, X.21 de 8 puertos, HSSI de 1 puerto y de circuitos de marcación
Frame Relay	Interfaces V.24/EIA 232E de 8 puertos, V.35/V.36 de 6 puertos, X.21 de 8 puertos, HSSI de 1 puerto y de circuitos de marcación
X.25	Adaptadores V.24/EIA 232E de 8 puertos, V.35/V.36 de 6 puertos y X.21 de 8 puertos
SDLC Relay	V.24/EIA 232E de 8 puertos, V.35/V.36 de 6 puertos y X.21 de 8 puertos
SDLC	Interfaces V.24/EIA 232E de 8 puertos, V.35/V.36 de 6 puertos, X.21 de 8 puertos y de circuitos de marcación
V.25bis	V.24/EIA 232E de 8 puertos
Marcación de entrada	Una interfaz de circuito de marcación PPP que tiene parámetros de configuración que toman valores por omisión para dar soporte a DIAL

Tabla 3. Arquitectura de red e interfaces soportadas (continuación)

Arquitectura de red	Interfaces soportadas
PPP de múltiples enlaces (MP)	Soportado en cualquier enlace PPP
Adaptador de canal ESCON	Estación de canal LAN (LCS), Arquitectura de servicios de enlace (LSA) y Canal de diversas vías de acceso+ (MPC+)
Adaptador de canal paralelo	Estación de canal LAN (LCS), Arquitectura de servicios de enlace (LSA) y Canal de diversas vías de acceso+ (MPC+)
L2TP, L2F y PPTP	Soporta conexiones virtuales PPP DIALs a través de los protocolos Layer 2 Tunneling Protocol (L2TP), Layer 2 Forwarding (L2F) y Point to Point Tunneling Protocol (PPTP).
FDDI	FDDI de 1 puerto

Notas:

1. Las interfaces de circuito de marcación PPP pueden utilizar RDSI o V.25bis como interfaz de red base.
2. Las interfaces de circuitos de marcación FR pueden utilizar RDSI o una red V.25bis como interfaz de red base.
3. Las interfaces de circuitos de marcación pueden utilizar una red RDSI como interfaz de red base.
4. Los circuitos de marcación SDLC utilizan V.25bis como interfaz de red base.

Acceso al proceso de consola de interfaz de red

Para supervisar la información relacionada con un dispositivo específico, acceda al proceso de consola utilizando el procedimiento siguiente:

1. En el indicador OPCON, entre el mandato **console**. Por ejemplo:
* console
2. Se visualiza el indicador GWCON (+) en la consola. Si no aparece el indicador cuando entra en GWCON, pulse **Intro** de nuevo.
3. En el indicador GWCON, entre el mandato **configuration**. Por ejemplo:

+configuration

Multiprotocol Access Services

2216-MAS Feature 2822 V3.2 Mod 0 PTF 0 RPQ 0 MAS.EF9 cc4_2a

```

Num Name Protocol
0 IP DOD-IP
3 ARP Address Resolution
4 DN DNA Phase IV
6 VIN Banyan Vines
7 IPX NetWare IPX
10 BGP Border Gateway Protocol
11 SNMP Simple Network Management Protocol
12 OSPF Open SPF-Based Routing Protocol
22 AP2 AppleTalk Phase 2
23 ASRT Adaptive Source Routing Transparent Enhanced Bridge
26 DLS Data Link Switching
27 XTP X.25 Transport Protocol
28 APPN Advanced Peer-to-Peer Networking [HPR]
30 APPN Advanced Peer-to-Peer Networking [ISR]

```

```

Num Name Feature
2 MCF MAC Filtering

```

16 Networks:

Net	Interface	MAC/Data-Link	Hardware	State
0	TKR/0	Token-Ring/802.5	Token-Ring	Up
1	TKR/1	Token-Ring/802.5	Token-Ring	Up
2	TKR/2	Token-Ring/802.5	Token-Ring	Up
3	TKR/3	Token-Ring/802.5	Token-Ring	Up
4	Eth/0	Ethernet/IEEE 802.3	Ethernet	Up
5	Eth/1	Ethernet/IEEE 802.3	Ethernet	Up
6	Eth/2	Ethernet/IEEE 802.3	Ethernet	Up
7	Eth/3	Ethernet/IEEE 802.3	Ethernet	Up
8	Eth/4	Ethernet/IEEE 802.3	Ethernet	Up
9	Eth/5	Ethernet/IEEE 802.3	Ethernet	Up
10	FR/0	Frame Relay	V.35/V.36	Up
11	X25/0	X.25	V.35/V.36	Up
12	PPP/0	Point to Point	V.35/V.36	Up
13	PPP/1	Point to Point	V.35/V.36	Up
14	PPP/2	Point to Point	V.35/V.36	Up
15	PPP/3	Point to Point	V.35/V.36	Up

4. Entre el mandato **network** de GWCON y el número de la interfaz que desea supervisar. Por ejemplo:

```
+ network 11
X.25>
```

En este ejemplo, se visualiza el indicador de consola X.25 en la consola. Puede ver información acerca de la interfaz X.25 entrando los mandatos de consola X.25.

Supervisión de la interfaz de red: Consulte los capítulos específicos de este manual para ver información completa sobre la supervisión de las interfaces de red del 2216.

Acceso a los procesos de configuración y operación de características

Para ayudarle a acceder a los procesos de configuración y operación de la característica Multiprotocol Access Services, esta sección le indica ambos procedimientos.

Acceso a los procesos de características

Utilice el mandato **feature** del proceso CONFIG para acceder a los mandatos de configuración para las características específicas de Multiprotocol Access Services que se encuentran fuera de los procesos de configuración de la interfaz de red y del protocolo.

Utilice el mandato **feature** desde el proceso GWCON para acceder a los mandatos de consola para las características específicas que se encuentran fuera de los procesos de consola de la interfaz de red y del protocolo.

Entre un signo de interrogación después del mandato **feature** para visualizar un listado de las características disponibles para el release de software. Por ejemplo:

```
Config> feature ?
WRS
BRS
MCF
TSF
Feature name or number [1] ?
```

Para acceder a un indicador en particular de configuración o de operación de una característica, entre el mandato **feature** en el indicador Config> o + (GWCON), respectivamente, seguido del número de la característica o del nombre corto. Por ejemplo:

```
Config> feature mcf
MAC filtering user configuration
Filter Config>
```

La Tabla 9 en la página 97 lista los números y nombres de características disponibles.

Tras acceder al indicador de configuración o de operación para una característica, puede empezar a entrar los mandatos específicos para esta característica. Para volver al nivel anterior de indicador, entre el mandato **exit** en el indicador de la característica.

Acceso a los procesos de configuración y operación de protocolos

Esta sección describe cómo acceder a los procesos de configuración y operación de protocolos.

Entrada en un proceso de configuración de protocolo

Para entrar en el proceso de configuración del protocolo deseado desde el indicador CONFIG>:

1. En el indicador CONFIG>, entre el mandato **list configuration** para ver los números y los nombres de los protocolos adquiridos que hay en la copia de software. Consulte la página 98 para ver un ejemplo de salida del mandato **list configuration**.
2. En el indicador Config>, entre el mandato **protocol** con el número o el nombre corto (por ejemplo, SNMP) del protocolo que desea configurar. El número y nombre corto del protocolo se obtienen con la visualización del mandato **list configuration**. En el ejemplo siguiente, se ha entrado el mandato para acceder al proceso de configuración del protocolo SNMP:

```
Config> protocol SNMP
O
Config> protocol 11
SNMP user configuration
```

Después, se visualiza el indicador de configuración del protocolo en la consola. El ejemplo siguiente muestra el indicador de configuración del protocolo SNMP:

```
SNMP config>
```

Ahora, puede empezar a entrar los mandatos de configuración del protocolo. Consulte la sección correspondiente al protocolo de la publicación *Consulta de configuración y supervisión de protocolos* para obtener más información sobre los mandatos de configuración específicos de protocolo.

En resumen, el mandato **protocol** le permite entrar en el proceso de configuración para el software de protocolo instalado en el dispositivo. El mandato **protocol** entra en el proceso de mandatos de un protocolo. Después de entrar el mandato **protocol**, aparece el indicador del protocolo especificado. En el indicador, puede entrar los mandatos específicos de ese protocolo.

Entrada en un proceso de operación de protocolo

Para entrar en un proceso de consola de protocolo desde el indicador GWCON:

1. En el indicador GWCON, entre el mandato **configuration** para ver los protocolos y las redes configurados para el dispositivo. Por ejemplo:

+configuration

Multiprotocol Access Services

```
2216-MAS Feature 2822 V3.2 Mod 0 PTF 0 RPQ 0 MAS.EF9 cc4_2a
Num Name Protocol
0 IP DOD-IP
3 ARP Address Resolution
4 DN DNA Phase IV
6 VIN Banyan Vines
7 IPX NetWare IPX
10 BGP Border Gateway Protocol
11 SNMP Simple Network Management Protocol
12 OSPF Open SPF-Based Routing Protocol
22 AP2 AppleTalk Phase 2
23 ASRT Adaptive Source Routing Transparent Enhanced Bridge
26 DLS Data Link Switching
27 XTP X.25 Transport Protocol
28 APPN Advanced Peer-to-Peer Networking [HPR]
30 APPN Advanced Peer-to-Peer Networking [ISR]
```

```
Num Name Feature
2 MCF MAC Filtering
```

16 Networks:

Net	Interface	MAC/Data-Link	Hardware	State
0	TKR/0	Token-Ring/802.5	Token-Ring	Up
1	TKR/1	Token-Ring/802.5	Token-Ring	Up
2	TKR/2	Token-Ring/802.5	Token-Ring	Up
3	TKR/3	Token-Ring/802.5	Token-Ring	Up
4	Eth/0	Ethernet/IEEE 802.3	Ethernet	Up
5	Eth/1	Ethernet/IEEE 802.3	Ethernet	Up
6	Eth/2	Ethernet/IEEE 802.3	Ethernet	Up
7	Eth/3	Ethernet/IEEE 802.3	Ethernet	Up
8	Eth/4	Ethernet/IEEE 802.3	Ethernet	Up
9	Eth/5	Ethernet/IEEE 802.3	Ethernet	Up
10	FR/0	Frame Relay	V.35/V.36	Up
11	X25/0	X.25	V.35/V.36	Up
12	PPP/0	Point to Point	V.35/V.36	Up
13	PPP/1	Point to Point	V.35/V.36	Up
14	PPP/2	Point to Point	V.35/V.36	Up
15	PPP/3	Point to Point	V.35/V.36	Up

Nota: APPN® es una marca registrada de IBM.

- Entre el mandato **protocol** de GWCON con el número de protocolo o nombre corto del protocolo deseado que se visualiza en la información de configuración. En el ejemplo siguiente, se ha entrado el mandato para acceder al proceso de consola del protocolo SNMP.

```
+ protocol 11
```

```
0
```

```
+ protocol SNMP
```

Después, se visualiza el indicador de consola del protocolo en la consola. Este ejemplo muestra el indicador de consola del protocolo SNMP:

```
SNMP>
```

Ahora, puede empezar a entrar los mandatos del protocolo. Consulte la sección correspondiente al protocolo de la publicación *Consulta de configuración y supervisión de protocolos* para obtener más información acerca de los mandatos de consola específicos de protocolo.

Finalización del mandato

La función de finalización automática del mandato le ayuda en la sintaxis de los mandatos entrados en la línea de mandatos.

Para ilustrar el comportamiento de la Finalización de mandatos, suponga que los mandatos siguientes están permitidos en un contexto de menús determinado. (Sólo se trata de un menú de ejemplo.)

enable

auto-refresh

caching

set

cache-size

cache-timeout

priority

- Si escribe **ena** y pulsa la barra espaciadora, aparece todo el mandato **ENABLE**. Si ahora escribe **?**, aparece una lista de elementos que se pueden habilitar (**auto-refresh** y **caching**) y el mandato **ENABLE** permanece en la línea de mandatos.
- Si escribe **ena** y pulsa **Intro**, aparece un mensaje que indica que el mandato no se ha especificado del todo y una lista de los posibles elementos que se pueden habilitar (**auto-refresh** y **caching**) y el mandato **ENABLE** permanece en la línea de mandatos.
- Puesto que el mandato **ENABLE** necesita habilitar un elemento, aparece en una lista de posibles finalizaciones del mandato con “...” en el margen izquierdo para indicar que es necesario entrar más información para el mandato.
- Si la entrada coincide con varios mandatos, se visualiza una lista de finalizaciones posibles. La entrada en la nueva línea de mandatos se amplía al prefijo común más largo. Por ejemplo, si entra **set ca** y después pulsa la barra espaciadora, se listarán **CACHE-SIZE** y **CACHE-TIMEOUT** y la nueva línea de mandatos se ampliará a **SET cache-**, ya que “cache-” es común a las dos finalizaciones posibles. Ahora debe escribir la letra “s” o la letra “t” para distinguir entre las finalizaciones posibles “size” o “timeout”.
- A veces, los mandatos comunes aparecen en un formato alternativo (**SHOW**, **DISPLAY**, **LIST**). Si la Finalización de mandatos no llega a ninguna coincidencia de un mandato común, por ejemplo, **SHOW**, se visualizarán las alternativas **DISPLAY** o **LIST**, si se encuentran.
- Si la búsqueda de un mandato (y alternativos) no da como resultado una coincidencia exacta, se presenta una lista de finalizaciones posibles, utilizando parte de la entrada. Por ejemplo, **enable** seguido de la barra espaciadora se sustituiría por **ena** y se listaría **ENABLE** como finalización posible.
- Cuando aparece una lista de mandatos posibles, puede utilizar el tabulador para ir de uno a otro sucesivamente en la línea de mandatos actual. Puede utilizar la barra espaciadora o la tecla **Intro** para seleccionar el mandato mostrado.

Ayuda en línea cuando la finalización de mandatos está habilitada

La siguiente ayuda en línea está disponible cuando se habilita la finalización de mandatos.

Consulte la página 95 para ver la sintaxis de **enable command-completion**.

? El signo de interrogación visualiza una lista de finalizaciones posibles. Si el mensaje ya se ha completado, aparece un mensaje.

Barra espaciadora

Intenta completar la palabra actual de la línea de mandatos. Si no se encuentra una coincidencia exclusiva, se listan las finalizaciones posibles.

Tabulador

Intenta completar la palabra actual de la línea de mandatos. Si no se encuentra una coincidencia exclusiva, se listan las finalizaciones posibles y se puede pasar de una finalización a otra sucesivamente utilizando el tabulador. Utilice la barra espaciadora o la tecla Intro para seleccionar el mandato visualizado actualmente.

Intro

Intenta completar la palabra actual de la línea de mandatos. Si el mandato está completado, Intro ejecuta el mandato y lo almacena en el Histórico de mandatos. Si el mandato no está completo, se visualiza una lista de finalizaciones posibles.

Control-P

Vuelve al indicador de consola de operador MOS (*). (Control-P es el carácter de interceptación por omisión.)

Retroceso

Suprime el último carácter de la línea de mandatos.

Control-W

Suprime la última palabra de la línea de mandatos.

Control-U

Termina anormalmente el mandato actual.

Control-L

Renueva la línea de mandatos actual para visualizar su contenido.

Control-B

Recupera en sentido inverso. Sustituye la línea de mandatos actual por el mandato anterior del Histórico de mandatos circular.

Control-F

Recupera hacia adelante. Sustituye la línea de mandatos actual por el siguiente mandato del Histórico de mandatos.

Control-R

Señala el inicio de una secuencia de repetición en el Histórico de mandatos. Se utiliza con la función **Control-N**.

Control-N

Sustituye la línea de mandatos actual por el siguiente mandato de la secuencia de repetición cuyo mandato inicial se ha señalado con **Control-R**.

Control-C

Cancela Easy-Start, si está activado.

Escape ?

Escape, seguido de "?" imprime esta Ayuda de línea de mandatos:

Se aplican las normas siguientes a la finalización automática de mandatos:

- Los mandatos completados aparecen en MAYÚSCULAS en la línea de mandatos.
- A veces, los mandatos comunes aparecen en formato alternativo (**ADD** en vez de **CREATE**). Si la finalización de mandatos no da como resultado una coincidencia de un mandato común, se visualizará cualquier mandato alternativo.
- Si la búsqueda de un mandato (y mandatos alternativos) no da como resultado una coincidencia exclusiva, aparece una lista de finalizaciones posibles y se presenta el prefijo común más largo.

- Cuando se listan finalizaciones posibles, los mandatos que necesitan que se entre más información aparecen con “...” en el margen izquierdo.
- Cuando se pulsa una tecla de recuperación del Histórico de mandatos (Control-B,F,N), se explora el Histórico de mandatos en busca de un mandato que se analice satisfactoriamente en el contexto del mandato actual. Sonará un pitido si no existe ningún mandato.
- Algunos mandatos de menú se crean dinámicamente. La Finalización de mandatos no puede seguir siempre estos enlaces dinámicos. Se puede entrar '?' en estos casos.
- Para inhabilitar la Finalización de mandatos para un solo mandato (para entrar un comentario), escriba cualquier Carácter de comentario como primer carácter de la línea de mandatos. Los Caracteres de comentario son !@#\$%^*.;/”
- La Finalización de mandatos se inhabilitará en caso de error interno. Proporcione la información de depuración de la pantalla al Soporte al cliente.
- La Finalización de mandatos está Habilitada actualmente. Para inhabilitar esta opción, utilice el mandato **disable command-completion** en talk 6 de la configuración.

Ayuda en línea cuando la finalización de mandatos está inhabilitada

La siguiente ayuda en línea está disponible cuando la finalización de mandatos está inhabilitada:

? Cuando se entra ? (signo de interrogación) al final de la línea de mandatos, aparece una lista de finalizaciones posibles.

Intro Ejecuta el mandato y lo almacena en el Histórico de mandatos. Aparece un mensaje si no se ha especificado completamente el mandato

Control-P

Vuelve al indicador de consola de operador MOS (*). (Control-P es el carácter de interceptación por omisión.)

Retroceso

Suprime el último carácter de la línea de mandatos.

Control-U

Termina anormalmente el mandato actual.

Control-B

Recupera en sentido inverso. Sustituye la línea de mandatos actual por el mandato anterior del Histórico de mandatos circular.

Control-F

Recupera hacia adelante. Sustituye la línea de mandatos actual por el siguiente mandato del Histórico de mandatos.

Control-R

Señala el inicio de una secuencia de repetición en el Histórico de mandatos. Se utiliza con la función **Control-N**.

Control-N

Sustituye la línea de mandatos actual por el siguiente mandato de la secuencia de repetición cuyo mandato inicial se ha señalado con **Control-R**.

Control-C

Cancela Easy-Start, si está activado.

Escape ?

Escape, seguido de “?” imprime esta Ayuda de línea de mandatos:

Command Completion is currently Disabled. To Enable this option, use the **enable command-completion** command from Configuration talk 6.

Histórico de mandatos

El Histórico de mandatos contiene hasta los últimos 50 mandatos entrados por el usuario en los menús de línea de mandatos OPCON, GWCON (Talk 5) o CONFIG (Talk 6).

Se pueden utilizar las teclas de recuperación hacia atrás y adelante para volver a llamar mandatos que se han entrado previamente. Además, se proporciona un recurso para permitir que el usuario avanzado repita una serie en particular de mandatos.

Repetición de un mandato del Histórico de mandatos

Si se pulsa **Control-B** (atrás) o **Control-F** (adelante) en cualquier indicador de línea de mandatos de los menús OPCON, GWCON o CONFIG, la línea de mandatos se sustituye por el mandato anterior o siguiente del Histórico de mandatos. El Histórico de mandatos es común en toda la interfaz de línea de mandatos. Es decir, un mandato que se ha entrado en un menú GWCON puede recuperarse desde CONFIG y un mandato que se ha entrado en un menú CONFIG puede recuperarse desde GWCON.

Cuando la Finalización de mandatos está habilitada (Consulte la sección "Finalización del mandato" en la página 23) y se pulsa una tecla de recuperación del Histórico de mandatos (Control-B,F,N), se explora el Histórico de mandatos en busca de un mandato que se analice satisfactoriamente en el contexto de mandatos actual. Sonará un pitido si no existe ningún mandato.

El Histórico de mandatos contiene los mandatos entrados más recientemente, hasta un máximo de los 50 últimos mandatos. Si sólo se han entrado tres mandatos desde que se ha vuelto a cargar, cuando se pulsa **Control-F** o **Control-B** se pasa sucesivamente por estos tres mandatos solamente. Si no se han entrado mandatos hasta ahora, **Control-F** o **Control-B** generan un pitido.

Nota: Los mandatos que se cancelan anormalmente mediante **Control-U** no se entrarán en el Histórico de mandatos. Cuando la Finalización de mandatos está habilitada, sólo se entran mandatos completos en el Histórico de mandatos.

Para entrar dos mandatos similares:

```
display sub les
display sub lec
```

Entre:

```
display sub les y, a continuación, pulse Intro
Control-B para retroceder y la línea actual se sustituye por -
display sub les
Pulse Retroceso y sustituya "s" por "c" para obtener
display sub lec y, a continuación, pulse Intro
```

Repetición de una serie de mandatos del Histórico de mandatos

Existe una característica adicional para usuarios avanzados que facilita la repetición de una serie en particular de mandatos GWCON o CONFIG. Se hace referencia a C1, C2,...,Cn del Histórico de mandatos como una *secuencia de repetición*. Esta característica puede ser más conveniente que simplemente utilizar **Control-B** y **Control-F** cuando se debe repetir una tarea determinada que necesita varios mandatos. Entre **Control-R** (repetición) para establecer el inicio de la *secuencia de repetición* en el mandato C1. Entre **Control-N** (siguiente) sucesivamente para recuperar el siguiente mandato de la secuencia de repetición. Los mandatos no se entran automáticamente, pero se colocan en la línea de mandatos actual permitiéndole modificar o entrar el mandato.

Para producir el comportamiento adecuado de una secuencia de repetición, el primer mandato recuperado utilizando el primer **Control-N** (siguiente) depende de la manera en que se ha establecido el inicio de la secuencia de repetición mediante **Control-R** (repetición).

El establecimiento del inicio de la secuencia de repetición con **Control-R** puede realizarse de dos maneras:

1. Cuando se entra C1 inicialmente
2. Cuando se recupera C1 del Histórico de mandatos mediante **Control-B** o **Control-F**.

Inicio de una secuencia de repetición a medida que se entran mandatos

Si entra **Control-R** cuando se está escribiendo el mandato C1 y después, entra los mandatos C2, C3... Cn. **Control-N** proporcionará los mandatos C1, C2, ... Cn, C1, C2, ... Cn, C1, ... sucesivamente en la línea de mandatos.

En el Ejemplo 1, el inicio de la secuencia de repetición se establece mientras se escribe el primer mandato. El usuario sabe de antemano que los mismos mandatos que se van a entrar en GWCON se han de repetir en CONFIG.

Ejemplo 1

1. Mientras escribe el primer mandato de la secuencia, utilice **Control-R** (repetición) para establecer el inicio de la secuencia de repetición.

```
*console
+event Control-R
```

después pulse **Intro** para establecer el inicio de la secuencia de repetición.

2. Continúe escribiendo los mandatos subsiguientes de la secuencia:

```
Event Logging System user console
ELS>display sub les
ELS>display sub lec
ELS>exit
+
```

3. Para entrar estos mismos mandatos en CONFIG, pulse **Control-P** (el carácter de interceptación de OPCON por omisión) y vaya a CONFIG.

```
+pulse Control-P-
*configuration
Config>Control-N por NEXT para recuperar el inicio de esta secuencia-
Config>event Intro
Event Logging System user configuration
ELS config>Control-N por NEXT para recuperar el siguiente mandato de
la secuencia-
```

```

ELS config>display sub les Intro
ELS config>Control-N por NEXT para recuperar el siguiente mandato de
la secuencia-
ELS config>display sub lec Intro
ELS config>Control-N por NEXT para recuperar el siguiente mandato de
la secuencia-
ELS config>exit Intro
Config>

```

Inicio de una secuencia de repetición después de haber entrado todos los mandatos

Por otro lado, si primero entra C1, C2, ... Cn y recupera C1 mediante **Control-B** o **Control-F**. Cuando se entra **Control-R** y se entra **Control-N** sucesivamente se obtienen los mandatos C2,..., Cn, C1, C2,..., Cn, C1,...,Cn en la línea de mandatos (consulte el Ejemplo 2). Se pasa por alto la primera aparición de C1 porque ya está disponible en la línea de mandatos en el momento en que se ha recuperado y no es necesario volverlo a llamar por el primer **Control-N**.

En el Ejemplo 2, se entran todos los mandatos y, después, se recupera el primer mandato de la secuencia que se ha de repetir. Se ha entrado una secuencia de mandatos en GWCON y se tiene que repetir la misma secuencia en CONFIG.

Ejemplo 2

1. Entre los mandatos siguientes en GWCON:

```

*console
+event
Event Logging System user console
ELS>display sub les
ELS>display sub lec
ELS>exit
+

```

2. Para entrar los mismos mandatos en CONFIG, pulse **Control-P** (el carácter de interceptación de OPCON) y vaya a CONFIG.

```

+Control-P-
*configuration
Config>Control-B cuatro veces para recuperar el inicio de
la secuencia de los cuatro mandatos de este ejemplo-
Config>event
Config>event Control-R por REPEAT para establecer el inicio de la secuencia
de repetición-
Config>event Intro
Event Logging System user configuration
ELS config>Control-N por NEXT para recuperar el siguiente mandato de
la secuencia-
ELS config>display sub les Intro
ELS config>Control-N por NEXT para recuperar el siguiente mandato de
la secuencia-
ELS config>display sub lec Intro
ELS config>Control-N por NEXT para recuperar el siguiente mandato de
la secuencia-
ELS config>exit Intro
Config>

```

Capítulo 3. Acceso al firmware desde la interfaz de línea de mandatos

Esta sección explica las opciones de arranque que se pueden establecer desde el indicador de mandatos del firmware y de operación. Para obtener información acerca de la transferencia y la gestión de archivos, consulte la publicación *IBM 2216 Nways Multiaccess Connector Installation and Initial Configuration Guide*.

El 2216 está diseñado para arrancar desde uno de los bancos de imágenes integrados. Con la unidad de disco duro instalada, el 2216 tiene dos bancos de imágenes instalados que se pueden utilizar para IML o arrancar el dispositivo. El 2216 también tiene opciones para activarse en modalidad Atendida o Autónoma. La modalidad atendida necesita la interacción directa de un usuario en una consola conectada al puerto serie.

El dispositivo puede arrancarse desde la unidad de disco duro, conocida como Banco A y B.

Acceso al indicador del firmware

Antes de arrancar el direccionador, tenga en cuenta que:

- Necesita un terminal o una estación de trabajo IP conectado al 2216. Puede ser un dispositivo TTY VT100 conectado directamente a través del puerto serie. Puede conectar una estación de trabajo IP utilizando SLIP para conectarse al 2216. La dirección IP por omisión del 2216 es 10.1.1.2 y la dirección de la estación de trabajo debe ser 10.1.1.3.

Importante: Para acceder al indicador del firmware, puede detener el arranque del 2216. Para detenerlo, debe tener una consola TTY conectada directamente al puerto serie. Cuando el 2216 empiece su proceso de arranque, pulse **Control-C** en la consola para interrumpir la secuencia de arranque.

Otra manera de controlar el arranque es configurar el 2216 para que se active en modalidad atendida. La modalidad atendida puede configurarse desde el conjunto de mandatos del firmware.

Opciones de arranque disponibles para el 2216

El 2216 puede configurarse para la modalidad autónoma. En modalidad autónoma, debe haber elegido la imagen de carga y la configuración que se han de cargar. Se proporcionan dos bancos entre los que puede elegir. La estructura de los bancos de imágenes es la siguiente:

- IMAGEN - Estado de la imagen
- CONFIG 1 - Estado de Config
- CONFIG 2 - Estado de Config
- CONFIG 3 - Estado de Config
- CONFIG 4 - Estado de Config

Consulte la sección "List" en la página 57 para ver una descripción de los estados de archivos.

Modalidad atendida

Cuando el 2216 está configurado para activarse en modalidad atendida, se otorga al usuario el acceso al conjunto de mandatos del firmware. Desde este nivel de mandatos, puede seleccionar el Banco de imágenes desde el que se ha de realizar la carga y la configuración. Llegado este momento, puede cargar nuevos archivos de configuración o archivos de imágenes. Esta conexión es una conexión TTY o Telnet. Puede transferir archivos utilizando el protocolo Xmodem para TTY o TFTP para conexiones IP.

Importante: En el release 2, varios módulos de carga forman una sola carga de dispositivo. Si está transfiriendo una carga a un banco utilizando XMODEM, debe transferir los archivos individualmente. Se aplica lo siguiente:

1. Primero transfiera LML.Id
2. Debe asegurarse de que todos los archivos que forman la carga se transfieren satisfactoriamente. Cuando se produzca un error al transferir un archivo, recibirá el recuadro de mensaje "ERROR WRITING FILE". De lo contrario, puede suponer que el archivo se ha transferido satisfactoriamente.
3. Cuando se hayan transferido todos los archivos, el estado del banco cambiará de "Corrupt" a "Avail".

En modalidad atendida, puede empezar el arranque del 2216 pulsando **F9** o **<Esc>9** para iniciar el sistema operativo.

Modalidad autónoma

Es la modalidad normal para el 2216. Se activará en la imagen Activa, Local o Pendiente y la configuración basada en su selección.

Capítulo 4. Proceso y mandatos OPCON

Este capítulo describe los mandatos de configuración y de operación de la interfaz OPCON. Incluye las secciones siguientes:

- “¿Qué es el proceso OPCON?”
- “Acceso al proceso OPCON”
- “Mandatos OPCON”

¿Qué es el proceso OPCON?

El proceso de Consola de operador (OPCON) es el proceso a nivel raíz de la interfaz de usuario del software de dispositivo. La función principal de OPCON es comunicarse con los procesos de nivel secundario como, por ejemplo, Configuración, Consola y Anotación cronológica de sucesos. Mediante los mandatos OPCON, también puede:

- Visualizar información acerca del uso de memoria del dispositivo
- Volver a cargar el software de dispositivo (rearrancar)
- Ejecutar telnet o ping para otros dispositivos o sistemas principales
- Visualizar la información de estado de todos los procesos de dispositivo
- Manipular la salida de un proceso
- Cambiar el carácter de interceptación de OPCON

Acceso al proceso OPCON

Cuando se inicia por primera vez el dispositivo, aparece un mensaje de arranque en la consola. Después aparece el indicador OPCON (*) en la consola, indicando que el proceso OPCON está activado y preparado para aceptar mandatos.

El proceso OPCON le permite configurar, cambiar y supervisar todos los parámetros operativos del dispositivo. Mientras está en el proceso OPCON, el dispositivo reenvía tráfico de datos. Cuando se arranca el dispositivo y entra en OPCON, aparece un logotipo de copyright y un indicador de asterisco (*) en el terminal de consola conectado localmente. Se trata del indicador OPCON (OPerator's CONsole), la interfaz de usuario principal que permite acceder a los procesos de segundo nivel.

Algunos cambios realizados en los parámetros operativos del dispositivo mientras se está en OPCON surten efecto inmediatamente sin necesidad de reinicializar el dispositivo. Si los cambios no surten efecto, utilice el mandato **reload** en el indicador *.

En el indicador *, un extenso conjunto de mandatos le permite comprobar el estado de los diversos procesos de software internos, supervisar el rendimiento de las interfaces del dispositivo y los reenviadores de paquetes y configurar varios parámetros operativos.

Mandatos OPCON

Esta sección describe los mandatos OPCON. Los mandatos que se necesitan con más frecuencia aparecen antes del separador “- - -”. Cada mandato incluye una descripción, los requisitos de su sintaxis y un ejemplo. Los mandatos OPCON se resumen en la Tabla 4 en la página 34. Para utilizarlos, acceda al proceso OPCON y entre el mandato adecuado en el indicador OPCON (*).

Tabla 4. Mandatos OPCON

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página 10.
Configuration*	Accede al proceso de configuración del dispositivo. (talk 6)
Console*	Accede al proceso de consola del dispositivo. (talk 5)
Event Logging System*	Accede al proceso de anotación cronológica de sucesos. (talk 2)
ELS Console*	Accede al proceso de Consola ELS secundario del dispositivo. (talk 7)
Logout	Desconecta una consola remota.
Ping	Ejecuta ping en una dirección IP especificada.
Reload	Vuelve a cargar el dispositivo.
Telnet	Conecta con otro dispositivo.
-----	-----
Diags	Visualiza el estado del dispositivo y el contenido de la anotación cronológica de pruebas de hardware y del registro de errores del hardware.
Divert	Envía la salida de un proceso a una consola o a otro terminal.
Flush	Desecha la salida de un proceso.
Halt	Suspende la salida de un proceso.
Intercept	Establece el carácter de interceptación por omisión de OPCON.
Memory	Informa del uso de la memoria del dispositivo.
Status	Muestra información acerca de todos los procesos de dispositivos.
Suspend	Inhabilita temporalmente la Finalización de mandatos únicamente para la sesión actual.
Talk	Conecta con otro proceso de dispositivo y habilita el uso de sus mandatos.

* Cuando utilice este mandato por primera vez, se le recordará que puede utilizar **Control-P** para volver al indicador de Consola de operador MOS (*).

Configuration

Utilice el mandato **configuration** para acceder al proceso de configuración del dispositivo (talk 6). Consulte la sección “Capítulo 7. El proceso CONFIG (CONFIG - Talk 6) y sus mandatos” en la página 67 para obtener más información.

Sintaxis:

configuration

Ejemplo:

* **configuration**

(To return to the MOS Operator Console prompt (*), press Control-P)

```
Gateway user configuration
```

```
Config>
```

Console

Utilice el mandato **console** para acceder a la consola y al proceso de supervisión del dispositivo (talk 5). Consulte la sección “Capítulo 8. El proceso de operación/supervisión (GWCON - Talk 5) y sus mandatos” en la página 117 para obtener más información.

Sintaxis:

console

Ejemplo:

* **console**

CGW Operator Console

+

Diags

Utilice el mandato **diags** para visualizar el menú principal de los diagnósticos. Los menús de los diagnósticos le permiten habilitar, inhabilitar y probar los adaptadores o los puertos del hardware. Los menús de los diagnósticos tienen ayuda en pantalla para las diversas opciones y la información de estado que está disponible.

Puede utilizar la tecla "b" (retroceso) para volver a cualquier menú anterior. Utilice la tecla "e" (salir) para salir de los diagnósticos y volver al indicador de mandatos OPCON.

Consulte la publicación *Service and Maintenance Manual* para el 2216 para obtener más información sobre el soporte de diagnóstico.

Sintaxis:

diags

Divert

Utilice el mandato **divert** para enviar la salida de un proceso especificado a un terminal especificado. Este mandato le permite desviar la salida de varios procesos al mismo terminal para ver simultáneamente la salida. Normalmente, el mandato **divert** se utiliza para redireccionar los mensajes de salida MONITR a un terminal específico. El dispositivo sólo permite redireccionar determinados procesos.

El mandato **divert** necesita el PID y númerotty (número del terminal de salida). Para obtener estos valores, utilice el mandato **status** de OPCON. El número de terminal puede ser el número de la consola local (tty0) o de una de las consolas remotas (tty1, tty2). El ejemplo siguiente muestra los mensajes del Sistema de anotación cronológica de sucesos generados por el proceso MONITR (2) que se están enviando a la consola remota *tty1* (1).

Los mensajes de sucesos se visualizan inmediatamente aunque esté escribiendo un mandato. La pantalla y el teclado tienen almacenamientos intermedios independientes para evitar la confusión de mandatos. El ejemplo siguiente muestra el proceso MONITR conectado a TTY0 después de ejecutar el mandato **divert 2 0**. Si desea detener la salida, entre **halt 2**. El mandato **halt** se describe en la sección "Halt" en la página 37.

Sintaxis:

divert *pid númerotty*

Ejemplo:

Copyright Notices:
Copyright IBM Corp. 1994, 1997
MOS Operator Console

For help using the Command Line Interface, press ESCAPE, then '?'

```

* divert 2 0

* status
Pid Name      Status TTY  Comments
1  COpCN1    IOW  TTY0 gzs
2  Monitr    IDL  TTY0
3  Tasker    RDY  --
4  MOSDBG    DET  --
5  CGWCon    DET  --
6  Config    DET  --
7  ELSCon    DET  --
8  ROpCN1    IDL  TTY1
9  ROpCN2    RDY  TTY2 jlg@128.185.40.40

```

Els

Utilice el mandato **els** para acceder al proceso de consola ELS secundario del dispositivo, (talk 7). Consulte la sección “Acceso al proceso de consola ELS secundario, ELSCon (Talk 7)” en la página 15 para obtener más información.

Sintaxis:

els

Event

Utilice el mandato **event** para acceder al proceso de anotación cronológica de sucesos del dispositivo, (talk 2). Consulte la sección “Capítulo 10. Utilización del Sistema de anotación cronológica de sucesos (ELS)” en la página 137 para obtener más información.

Sintaxis:

event

Flush

Utilice el mandato **flush** para borrar los almacenamientos intermedios de salida de un proceso. Generalmente, este mandato se utiliza antes de visualizar el contenido del almacenamiento intermedio FIFO de MONITR para evitar que los mensajes se desplacen fuera de la pantalla. Se eliminan los mensajes acumulados.

El dispositivo sólo permite la eliminación de determinados procesos. Para obtener el PID y numerotty, utilice el mandato **status** de OPCON. En el ejemplo siguiente, después de ejecutar el mandato **flush 2**, se envía la salida del proceso MONITR al Destino (se ha eliminado).

Sintaxis:

flush *pid*

Ejemplo:

```

* flush 2
* status
Pid Name      Status TTY  Comments
1  COpCN1    IOW  TTY0
2  Monitr    IDL  SNK
3  Tasker    RDY  --
4  MOSDBG    DET  --
5  CGWCon    DET  --
6  Config    DET  --
7  ELSCon    DET  --
8  ROpCN1    IDL  TTY1
9  ROpCN2    RDY  TTY2 jlg@128.185.40.40

```

Halt

Utilice el mandato **halt** para suspender toda la salida subsiguiente de un proceso especificado hasta que se emita el mandato **divert**, **flush** o **talk** de OPCON para el proceso. El dispositivo no puede redireccionar todos los procesos. **Halt** es el estado por omisión para la salida de un proceso. Para obtener el PID para este mandato utilice el mandato **status** de OPCON. En el ejemplo siguiente, después de ejecutar el mandato **halt 2**, el proceso MONITR ya no está conectado a TTY0. Los mensajes de sucesos ya no aparecen más.

Sintaxis:

```
halt pid
```

Ejemplo:

```
* halt 2
* status
Pid  Name      Status TTY  Comments
1    COpCN1    IOW   TTY0 gzs
2    Monitr    IDL   --
3    Tasker    RDY   --
4    MOSDBG    DET   --
5    CGWCon    DET   --
6    Config    DET   --
7    ELSCon    DET   --
8    ROpCN1    IDL   TTY1
9    ROpCN2    RDY   TTY2 j1g@128.185.40.40
```

Intercept

Utilice el mandato **intercept** para cambiar el carácter de interceptación de OPCON. El carácter de interceptación es lo que se entra desde otros procesos para volver al proceso OPCON. La combinación de teclas de interceptación por omisión es **Control-P**.

El carácter de interceptación puede ser un carácter de control. Entre el carácter [^] (desplazamiento 6) seguido de una letra o de un carácter que no sea alfanumérico como, por ejemplo, !@#\$, que desee que sea el carácter de interceptación.

Nota: Este cambio sólo se aplica al inicio de sesión actual.

Sintaxis:

```
intercept carácter^
```

Ejemplo 1:

```
* intercept ^a
```

A partir de este ejemplo, el carácter de interceptación es **Control-A**.

Ejemplo 2:

```
* intercept !
```

A partir de este ejemplo, el carácter de interceptación es **!**.

Logout

Utilice el mandato **logout** para terminar la sesión actual para el usuario que entra el mandato logout. Si está habilitado el inicio de sesión de la consola, es posible que este mandato necesite que el próximo usuario que inicie la sesión utilice una

combinación autorizada de id de usuario/contraseña. Si el inicio de sesión no está habilitado, aparece de nuevo el indicador OPCON.

Sintaxis:

logout

Memory

Utilice el mandato **memory** para obtener y visualizar información acerca del uso de memoria de almacenamiento dinámico global del dispositivo. Su visualización le ayuda a determinar si el dispositivo se está utilizando de manera eficaz. Para ver un ejemplo de utilización de memoria, consulte la Figura 3.

Consulte la sección “Memory” en la página 127 para ver el uso de memoria mediante talk 5.

Sintaxis:

memory

Ejemplo:

```
* memory
Number of bytes: Busy = 319544, Idle = 1936, Free = 1592
```

Busy Especifica el número de bytes asignados actualmente.

Idle Especifica el número de bytes asignados previamente pero liberados y disponibles para volverlos a utilizar.

Free Especifica el número de bytes que nunca se han asignado del área de almacenamiento libre inicial.

Nota: La suma de la memoria Idle y Free es igual al total de memoria de almacenamiento dinámico disponible.

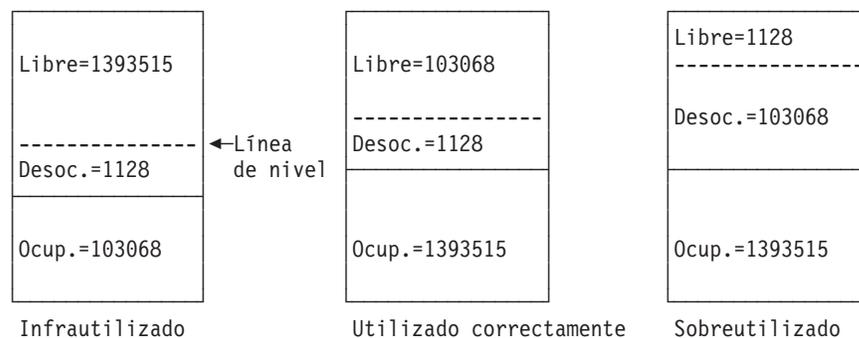


Figura 3. Utilización de la memoria

Ping

Utilice el mandato **ping** para que el dispositivo envíe los mensajes de eco ICMP a un destino determinado (es decir, “ejecutando ping”) y espere una respuesta. Este mandato puede utilizarse para identificar un problema entre redes.

Sintaxis:

ping

dir-dest [dir-scr tam-dat ttl vel tos valor-datos]

El proceso de ping se realiza continuamente, incrementando el número de secuencia ICMP con cada paquete adicional. Se informa de cada respuesta de eco ICMP coincidente que se recibe con su número de secuencia y el tiempo de ida y vuelta. La granularidad (resolución de tiempo) del cálculo de tiempo de ida y vuelta normalmente es de 20 milisegundos aproximadamente, dependiendo de la plataforma.

Para detener el proceso de ping, escriba cualquier carácter en la consola. En ese momento, se visualizará un resumen de la pérdida de paquetes, el tiempo de ida y vuelta y el número de destinos ICMP no alcanzados.

Cuando se da una dirección de difusión o de multidifusión como destino, pueden visualizarse múltiples respuestas para cada paquete enviado, uno para cada miembro del grupo. Se visualiza cada respuesta devuelta con la dirección de origen del que responde.

Puede especificar el tamaño de ping (número de bytes de datos del mensaje ICMP, excluyendo la cabecera ICMP), el valor de los datos, el valor del período de duración (TTL), la velocidad de ejecución de ping y los bits TOS que se han de establecer. También puede especificar la dirección IP de origen. Si no especifica la dirección IP de origen, el dispositivo utiliza la dirección local de la interfaz de salida para el destino especificado. Si valida la conectividad de cualquiera de las otras interfaces del dispositivo para el destino, entre la dirección IP para esa interfaz como dirección de origen.

Sólo es necesario el parámetro de destino; todos los demás parámetros son opcionales. Por omisión, el tamaño es de 56 bytes, el TTL es 64, la velocidad es 1 ping por segundo y el valor de TOS es 0. Los 4 primeros bytes de los datos ICMP se utilizan como indicación de la hora. Por omisión los datos restantes son una serie de bytes con valores que se incrementan en 1, empiezan por X'04' y van de forma cíclica de X'FF' a X'00' (por ejemplo, X'04 05 06 07 . . . FC FD FE FF 00 01 02 03 . . .'). Estos valores sólo se incrementan cuando se utiliza el valor por omisión; si se especifica el valor de byte de datos, todos los datos ICMP (excepto los 4 primeros bytes) se establecen en ese valor y no se incrementa. Por ejemplo, si establece el valor de byte de datos en X'FF', los datos ICMP son una serie de bytes con el valor X'FF FF FF . . .!.

Ejemplo:

```
* ping
Destination IP address [0.0.0.0]? 192.9.200.1
Source IP address [192.9.200.77]?
Ping data size in bytes [56]?
Ping TTL [64]?
Ping rate in seconds [1]?
Ping TOS (00-FF) [0]? e0
Ping data byte value (00-FF) [ ]?
PING 192.9.200.77-> 192.9.200.1:56 data bytes,ttl=64, every 1 sec.
56 data bytes from 192.9.200.1:icmp_seq=0.ttl=255.time=0.ms
56 data bytes from 192.9.200.1:icmp_seq=1.ttl=255.time=0.ms
56 data bytes from 192.9.200.1:icmp_seq=2.ttl=255.time=0.ms

----192.9.200.1 PING Statistics----
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max=0/0/0 ms
```

Reload

Utilice el mandato **reload** para rearrancar el dispositivo cargando una nueva copia del software de dispositivo. Cuando se utiliza este mandato desde una consola

remota, se instala una nueva carga de software sin ir al dispositivo. Este mandato ejecuta las mismas funciones que pulsar el botón de restablecimiento excepto en que el dispositivo no se volcará (si está configurado para ello). Antes de que volver a cargar surta, se solicita que lo confirme. También se solicita si no ha guardado los cambios en la configuración.

Sintaxis:

reload

Ejemplo:

```
* reload
Are you sure you want to reload the gateway (Yes or No)?
```

Status

Utilice el mandato **status** para visualizar la información acerca de todos los procesos de dispositivo. Mediante la introducción del PID después del mandato **status**, puede consultar el estado del proceso que desee solamente. El ejemplo siguiente muestra la visualización total del estado.

Sintaxis:

status *pid*

Ejemplo:

```
* status
Pid Name      Status TTY  Comments
1   COpCN1     IOW   TTY0
2   Monitr     IDL   --
3   Tasker     RDY   --
4   MOSDBG     DET   --
5   CGWCon     IOW   --
6   Config     IOW   TTY1
7   ELSCon     DET   --
8   ROpCN1     IOW   TTY1 128.185.46.101
9   ROpCN2     RDY   TTY2 128.185.46.104
```

Pid Especifica el PID. Es el proceso para conectarse desde OPCON o puede ser un argumento para que el mandato STATUS pida información de estado acerca de un proceso específico.

Name Especifica el nombre del proceso. Normalmente corresponde al nombre del programa que se ejecuta en el proceso.

Status

Especifica uno de los siguientes:

IDL Especifica que el proceso está desocupado y en espera de que finalice algún suceso externo como, por ejemplo, una E/S asíncrona.

RDY Especifica que el proceso está preparado para ejecutarse y en espera para utilizar la CPU.

IOW Especifica que el proceso está en espera de E/S síncrona, normalmente su entrada estándar esperada, para completarse.

DET Especifica que el proceso tiene la salida preparada para visualizarse y que está esperando conectarse a una consola de visualización o a que se desvíe su salida a una consola especificada.

FZN Especifica que el proceso está congelado debido a un error.

Normalmente significa que el proceso está intentando utilizar un dispositivo anómalo o configurado incorrectamente.

TTY n Especifica el terminal de salida, si lo hay, al que actualmente está conectado el proceso.

TTY0 Consola local

TTY1 o TTY2

Consolas Telnet.

Sink El proceso se ha eliminado.

Dos guiones (--)

El proceso se ha parado.

Comments

Especifica la dirección IP de inicio de sesión del usuario proporcionada durante el inicio de sesión de un usuario que utiliza Telnet (ROpCon).

Suspend

Utilice el mandato **suspend** para inhabilitar temporalmente la Finalización de mandatos sólo para la sesión actual. Si está utilizando un script automatizado, puede emitir **suspend yes** como el primer mandato si desea inhabilitar temporalmente la Finalización de mandatos.

Para obtener información acerca de la Finalización de mandatos, consulte la sección "Finalización del mandato" en la página 23.

Sintaxis:

suspend

Talk

Puede utilizar los mandatos **configuration**, **console** o **event** para conectarse a otros procesos como, por ejemplo, CONFIG, GWCON o MONITR, o puede utilizar el mandato **talk**. Después de conectarse a un nuevo proceso, puede enviar mandatos específicos y recibir salida de ese proceso. No puede conectarse a los procesos TASKER o OPCON.

Para obtener el PID, utilice el mandato **status** de OPCON. Una vez conectado al proceso de segundo nivel como, por ejemplo, CONFIG, utilice el carácter de interceptación **Control-P**, para volver al indicador *.

Sintaxis:

talk *pid*

Ejemplo:

* **talk** 5

CGW Operator Console

+

Cuando utilice procesos de tercer nivel como, por ejemplo, SNMP Config> o SNMP>, utilice el mandato **exit** para volver al segundo nivel.

Telnet

Utilice el mandato **telnet** para conectarse remotamente a otro dispositivo a un sistema principal remoto. El único parámetro opcional es el tipo de terminal que desea emular.

Puede utilizar el mandato **telnet** con las direcciones IPv4 o IPv6.

Un dispositivo tiene un máximo de cinco sesiones Telnet: dos servidores (entrada al dispositivo) y tres clientes (salida del dispositivo).

Nota: Para utilizar Telnet en un entorno de puente puro, habilite los Servicios del sistema principal.

Sintaxis:

telnet *dirección-ip tipo-terminal*

Ejemplo 1: telnet 128.185.10.30 o telnet 128.185.10.30 23 o telnet 128.185.10.30 vt100

```
Trying 128.185.10.30 ...
Connected to 128.185.10.30
Escape character is '^['
```

Ejemplo 2: telnet 1:9::10

```
Trying 1:9::10 ...
Connected to 1:9::10
Escape character is '^['
```

Cuando se ejecuta Telnet para una dirección IP inexistente, el dispositivo visualiza:

```
Trying 128.185.10.30 ...
```

Para entrar en la modalidad de mandatos Telnet, escriba la secuencia de caracteres de escape, que es **Control-]**, en cualquier indicador.

```
telnet>
```

Si ejecuta telnet en un dispositivo,

- Pulse **← Retroceso** para suprimir el último carácter escrito en la línea de mandatos.

Nota: Cuando utilice un terminal VT100, no pulse **← Retroceso** porque inserta caracteres invisibles. Pulse **Supr** para suprimir el último carácter.

- Pulse **Control-U** en el indicador telnet> para suprimir toda la entrada de la línea de mandatos y poder entrar un mandato de nuevo.

La modalidad de mandato Telnet consiste en los submandatos siguientes:

close Cierra la conexión actual

display

Visualiza los parámetros operativos

mode Intenta entrar en la modalidad de línea a línea o de un carácter cada vez

open Conecta a un sitio

quit Sale de Telnet

send Transmite caracteres especiales (send ? para más)

set Establece los parámetros operativos (set ? para más)

- status** Visualiza la información de estado
- toggle** Conmuta parámetros operativos (toggle ? para más)
- z** Suspende Telnet
- ?** Visualiza información de ayuda

Los submandatos **status** y **send** tienen dos respuestas dependiendo de si el usuario está conectado a otro sistema principal o no. Por ejemplo:

Conectado a un sistema principal:

```
telnet> status
Connected to 128.185.10.30  Operating in character-at-a-time mode.  Escape character is ^].

telnet> send ayt
```

Nota: Actualmente, el mandato send sólo soporta ayt.

No conectado a un sistema principal:

```
telnet> status
Need to be connected first.

telnet> send ayt

Need to be connected first.
```

Utilice el submandato **close** para cerrar una conexión con un sistema principal remoto y terminar la sesión Telnet. Utilice el submandato **quit** para salir de la modalidad de mandatos **telnet** y terminar una sesión Telnet.

```
telnet> close
```

O

```
telnet> quit

logout
*
```

Parte 2. Comprensión, configuración y utilización de los servicios básicos

Capítulo 5. Utilización de BOOT Config para efectuar la gestión de cambios

Este capítulo describe cómo utilizar el proceso Configuración de arranque/vuelco. Este capítulo incluye las secciones siguientes:

- “Comprensión de la gestión de cambios”
- “Utilización de Trivial File Transfer Protocol (TFTP)”
- “Carga de una imagen a una hora específica” en la página 49

Comprensión de la gestión de cambios

La gestión de cambios maneja los datos de software y de configuración para un IBM 2216. Esto implica:

1. Mover el código y los datos de configuración al IBM 2216 y desde el mismo
2. Mover el código y los datos de configuración del dispositivo de almacenamiento permanente del IBM 2216, que es una unidad de discos.
3. Seleccionar y activar combinaciones específicas de software y configuración.

Las funciones de la gestión de cambios están disponibles mediante la entrada del mandato **boot** en el indicador `Boot config>` (talk 6) o el firmware si la máquina está en una condición en la que la unidad de disco duro o la memoria instantánea compacta no contiene software viable (es decir, no puede acceder a talk 6).

El recurso de almacenamiento del código y los datos de configuración del IBM 2216 está dividido en áreas llamadas “bancos del sistema” (bancos para abreviar), cada uno de los cuales contiene una sola versión del código operativo y de cualquier otro archivo pertinente para ese release del código. Se asocian hasta cuatro archivos de configuración al software de cada banco.

El modelo de gestión de cambios general del IBM 2216 es introducir un nuevo código y/o datos de configuración en el sistema mientras éste se ejecuta en el presente nivel y activar el código o los datos de configuración cambiados que se han establecido con posterioridad. Si por alguna razón el nuevo código o configuración no funciona tal como se esperaba, tiene la posibilidad de revertir a la versión anterior de la configuración.

Utilización de Trivial File Transfer Protocol (TFTP)

TFTP es un protocolo de transferencia de archivos que se ejecuta a través del protocolo Internet UDP. Esta implementación proporciona múltiples transferencias de archivos TFTP simultáneas entre una memoria de configuración no volátil de un IBM 2216, el banco de imágenes y los sistemas principales remotos.

TFTP le permite:

- Obtener un archivo de configuración del servidor para un IBM 2216
- Poner un archivo de configuración de un IBM 2216 en un servidor
- Obtener módulos de carga de un servidor para un IBM 2216
- Poner módulos de carga de un IBM 2216 en un servidor

Las transferencias TFTP implican un nodo *cliente* y un nodo *servidor*. El nodo cliente genera una petición de obtener o poner TFTP en la red. El IBM 2216 actúa como nodo cliente generando peticiones TFTP desde la consola IBM 2216 utilizando el mandato **tftp** del proceso `Boot config>`.

Utilización de BOOT Config

El cliente puede transferir una copia de un archivo de configuración o un archivo de imágenes almacenado en el banco de imágenes de un servidor.

El servidor es cualquier dispositivo (por ejemplo, un personal computer o una estación de trabajo) que recibe y da servicio a las peticiones TFTP. Cuando el IBM 2216 actúa como servidor, las transferencias son transparentes para el usuario. Utilice la anotación cronológica de mensajes TFTP del subsistema ELS para ver la transferencia en proceso.

Transferencia de grandes cantidades de datos a múltiples archivos

Esta función es importante para las situaciones en las que el servidor TFTP receptor tiene un problema en el manejo del reinicio a cero de la cuenta de bloques o que tiene el valor 0x8000. El protocolo TFTP necesita la transmisión de una cuenta de bloques con cada bloque de datos. El reconocimiento de este bloque de datos transporta el número de bloque que estaba en el bloque de datos que se está reconociendo. El transmisor de los datos no enviará ningún dato más hasta que reciba un reconocimiento para el último bloque de datos enviado. Cuando el receptor de los datos envía el reconocimiento, espera recibir un bloque de datos con una cuenta de bloques que sea un número mayor que la cuenta de bloques que ha recibido previamente. Esta cuenta de bloques tiene dos bytes de longitud.

Algunos servidores TFTP tienen implementado incorrectamente esta función como una palabra corta con signo (variable de dos bytes en la que el bit de orden superior 1 indica un valor negativo) y otros como una palabra larga sin signo (variable de cuatro bytes).

Si la cantidad de datos que se ha de transferir es tan grande que la cuenta de bloques se reinicia, entonces dependiendo de la forma en que el receptor verifica la cuenta de bloques, puede reconocer los datos o no. Si el receptor utiliza una palabra corta con signo, el problema aparecerá cuando la cuenta de bloques pase de 0x7fff a 0x8000. Si el receptor utiliza una palabra larga o corta sin signo, el problema aparecerá cuando la cuenta de bloques pase de 0xffff a 0x0000. En ambos casos la cuenta de bloques del bloque de datos parecerá menor que la cuenta de bloques recibida previamente y el receptor se confundirá.

El TFTP transmisor del dispositivo recibirá un paquete de error o un tiempo de espera excedido cuando espere a que el receptor responda. Cuando ocurra esto, el TFTP del dispositivo se dará cuenta de que la cuenta de bloques se ha reiniciado y se recuperará automáticamente realizando una petición de grabación al receptor para un nuevo archivo. El nombre del nuevo archivo se deriva del nombre del archivo original. El nombre del nuevo archivo se deriva recubriendo los dos últimos caracteres del nombre de archivo original con dos dígitos decimales. Cada vez que se reinicia la cuenta de bloques, se grabará un nuevo archivo hasta que se hayan transferido todos los archivos. Se pueden utilizar herramientas como, por ejemplo, **cat** en el receptor para concatenar los archivos.

Especificación del número máximo de bloques que se han de transferir a un archivo del receptor

Se ha añadido una variable de parche para que pueda especificar el número máximo de bloques que se pueden transferir a un archivo del receptor. Esto le permite indicar al dispositivo que realice automáticamente una petición de grabación para un nuevo archivo una vez se haya enviado el número de bloques especificado. Al hacer esto se evita la recuperación automática descrita arriba, acelerando la transferencia, ya que se evita el período de tiempo de espera excedido de 5 minutos.

Los únicos valores que pueden especificarse para esta variable de parche son: 0xffff (65535) y 0x7fff (32767).

Esta variable de parche es útil cuando se sabe que el servidor receptor tiene problemas con el manejo del reinicio de la cuenta de bloques.

Carga de una imagen a una hora específica

Pueden haber ocasiones en que desee cargar un dispositivo en un día y hora específicos en los que el usuario no estará presente. Puede configurar el dispositivo para que realice una carga planificada utilizando el mandato **timeload activate**. Hay otros mandatos que le permiten ver la información de la carga planificada de un dispositivo o cancelar una carga planificada. Consulte la sección “Mandatos de configuración de la gestión de cambios” en la página 51 para obtener información sobre estos mandatos.

Capítulo 6. Configuración de la gestión de cambios

Este capítulo describe los mandatos para la configuración de la gestión de cambios. Incluye las secciones siguientes:

- “Acceso al entorno de configuración de la gestión de cambios”
- “Mandatos de configuración de la gestión de cambios”

Acceso al entorno de configuración de la gestión de cambios

Para entrar en el entorno de mandatos de configuración de la gestión de cambios utilice el mandato **boot** de CONFIG. Cuando se carga inicialmente el software del dispositivo, ejecuta el proceso OPCON, que señalado por el indicador *. En el indicador *:

1. Entre **talk 6**.
2. En el indicador `Config>`, escriba **boot**.

Para volver al proceso CONFIG, escriba **exit**.

Mandatos de configuración de la gestión de cambios

Esta sección describe los mandatos de la Configuración de la gestión de cambios. Cada mandato incluye una descripción, los requisitos de su sintaxis y un ejemplo. La Tabla 5 resume los mandatos de la Configuración de la gestión de cambios.

Después de acceder al entorno de la Configuración de la gestión de cambios, entre los mandatos de configuración en el indicador `Boot config>`.

Tabla 5. Mandatos de la Configuración de la gestión de cambios

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página 10.
Add	Añade una descripción opcional a un archivo de configuración.
Copy	Copia los archivos de arranque y los archivos de configuración a los bancos o de los mismos.
Describe	Visualiza información acerca de las imágenes de archivos de carga almacenadas.
Disable	Desactiva diversas funciones de la gestión de cambios.
Enable	Activa diversas funciones de la gestión de cambios.
Erase	Borra una imagen almacenada o un archivo de configuración.
List	Visualiza información acerca de archivos de configuración e información de carga planificada.
Lock	Impide que el dispositivo grabe una configuración encima de la configuración seleccionada.
Set	Selecciona el banco de códigos y la configuración que se ha de utilizar.
Tftp	Inicia las transferencias de archivos TFTP entre el IBM 2216 y los servidores remotos.
Timeload	Planifica una carga en el dispositivo para un día y hora específicos, cancela una carga planificada o visualiza información de carga planificada.
Unlock	Elimina el bloqueo de una configuración permitiendo que el dispositivo la actualice.

Tabla 5. Mandatos de la Configuración de la gestión de cambios (continuación)

Mandato	Función
Update Firmware	Instala el módulo de carga Firm.Id que ha recibido del Banco A o del Banco B en el 2216
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página 11.

Add

Utilice el mandato **add** para añadir una descripción opcional a un archivo de configuración.

Sintaxis:

```
add configuration archivo descripción
load imagen descripción
```

Ejemplo: Boot config> add

```
+----- BankA -----+----- Description -----+----- Date -----+
| IMAGE - NONE                |                               | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL            | test config for pubs         | 01 Jan 1970 01:26 |
| CONFIG 2 - AVAIL *          | test config for pubs         | 01 Jan 1970 01:13 |
| CONFIG 3 - AVAIL            |                               | 01 Jan 1970 01:39 |
| CONFIG 4 - AVAIL            |                               | 01 Jan 1970 01:52 |
+----- BankB -----+----- Description -----+----- Date -----+
| IMAGE - ACTIVE              |                               | 01 Jan 1970 00:30 |
| CONFIG 1 - AVAIL            | test config for pubs         | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL            |                               | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL            |                               | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE *         |                               | 01 Jan 1970 00:24 |
+-----+-----+-----+
* - Last Used Config      L - Config File is Locked
```

```
Select the source bank: (A, B): [A]
Select the source configuration: (1, 2, 3, 4): [1] 3
Enter the description of the file: () New config for today
```

Attempting to set description for bank A configuration 3.

Operation completed successfully.

Boot config>list

```
+----- BankA -----+----- Description -----+----- Date -----+
| IMAGE - NONE                |                               | 01 Jan 1970       |
| CONFIG 1 - AVAIL            | test config for pubs         | 01 Jan 1970 00:58 |
| CONFIG 2 - AVAIL *          | test config for pubs         | 01 Jan 1970 01:13 |
| CONFIG 3 - NONE             | New config for today         | 09 Jan 1970 00:58 |
| CONFIG 4 - AVAIL            |                               | 01 Jan 1970 01:05 |
+----- BankB -----+----- Description -----+----- Date -----+
| IMAGE - ACTIVE              |                               | 01 Jan 1970       |
| CONFIG 1 - AVAIL            | test config for pubs         | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL            |                               | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL            |                               | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE *         |                               | 01 Jan 1970 00:24 |
+-----+-----+-----+
* - Last Used Config      L - Config File is Locked
```

Auto-boot mode is enabled. Fast-boot mode is disabled.

Copy

Utilice el mandato **copy** para copiar los archivos de configuración y cargar las imágenes en los bancos y de los mismos.

Nota: Puede utilizar el mandato **copy bank** para copiar todo un banco, lo que es conveniente si desea utilizar un banco como copia de seguridad de otro banco.

Sintaxis:

```
copy                bank
                    configuration archivo
```

Ejemplo:

Boot config>**copy bank**

BankA	Description	Date
IMAGE - PENDING		22 Jan 1999 17:15
CONFIG 1 - AVAIL		05 Feb 1999 13:42
CONFIG 2 - PENDING *		22 Jan 1999 17:24
CONFIG 3 - AVAIL		05 Feb 1999 13:42
CONFIG 4 - AVAIL		05 Feb 1999 13:42
BankB	Description	Date
IMAGE - AVAIL		05 Feb 1999 13:39
CONFIG 1 - CORRUPT		05 Feb 1999 13:39
CONFIG 2 - AVAIL		05 Feb 1999 13:39
CONFIG 3 - AVAIL		05 Feb 1999 13:39
CONFIG 4 - AVAIL		05 Feb 1999 13:39

* - Last Used Config L - Config File is Locked

Auto-boot mode is disabled. Fast-boot mode is disabled.

```
Select the source bank: (A, B): [A] A
Select the destination bank: (A, B): [B] B
we are about to try copying configs
Copy SW configuration from: bank A, configuration 1
                           to: bank B, configuration 1.
/hd0/sys0/CONFIG0 --> /hd0/sys1/CONFIG0

Operation completed successfully.
Copy SW configuration from: bank A, configuration 2
                           to: bank B, configuration 2.
/hd0/sys0/CONFIG1 --> /hd0/sys1/CONFIG1
Operation completed successfully.
Copy SW configuration from: bank A, configuration 3
                           to: bank B, configuration 3.
/hd0/sys0/CONFIG2 --> /hd0/sys1/CONFIG2

Operation completed successfully.
Copy SW configuration from: bank A, configuration 4
                           to: bank B, configuration 4.
/hd0/sys0/CONFIG3 --> /hd0/sys1/CONFIG3

Operation completed successfully.

Copy SW load image from: bank A
                           to: bank B.
Operation completed successfully.
Boot config>
```

Ejemplo: Boot config>copy load

BankA	Description	Date
IMAGE - AVAIL		01 Jan 1970 00:01
CONFIG 1 - AVAIL	test config for pubs	01 Jan 1970 01:26
CONFIG 2 - AVAIL *	test config for pubs	01 Jan 1970 01:13
CONFIG 3 - AVAIL		01 Jan 1970 01:39
CONFIG 4 - AVAIL		01 Jan 1970 01:52

BankB	Description	Date
IMAGE - ACTIVE		01 Jan 1970 00:01
CONFIG 1 - AVAIL		01 Jan 1970 00:14
CONFIG 2 - AVAIL		01 Jan 1970 00:01
CONFIG 3 - AVAIL		01 Jan 1970 00:37
CONFIG 4 - ACTIVE *		01 Jan 1970 00:24

* - Last Used Config L - Config File is Locked

Select the source bank: (A, B): [A] b
Select the destination bank: (A, B): [B] a
Copy SW load image from: bank B
to: bank A.

Operation completed successfully.

Example: Boot config>copy

BankA	Description	Date
IMAGE - CORRUPT		01 Jan 1970 00:01
CONFIG 1 - AVAIL	test config for pubs	01 Jan 1970 01:26
CONFIG 2 - AVAIL *	test config for pubs	01 Jan 1970 01:13
CONFIG 3 - AVAIL		01 Jan 1970 01:39
CONFIG 4 - AVAIL		01 Jan 1970 01:52

BankB	Description	Date
IMAGE - ACTIVE		01 Jan 1970 00:01
CONFIG 1 - AVAIL		01 Jan 1970 00:14
CONFIG 2 - AVAIL		01 Jan 1970 00:01
CONFIG 3 - AVAIL		01 Jan 1970 00:37
CONFIG 4 - ACTIVE *		01 Jan 1970 00:24

* - Last Used Config L - Config File is Locked

Select the source bank: (A, B): [A]
Select the source configuration: (1, 2, 3, 4): [1]
Select the destination bank: (A, B): [B]

Select the destination configuration: (1, 2, 3, 4): [1]
Copy SW configuration from: bank A, configuration 1
to: bank B, configuration 1.
/hd0/sys0/CONFIG0 --> /hd0/sys1/CONFIG0

Operation completed successfully.

Si la copia falla, puede recibir uno de los mensajes siguientes:

Error: Active bank cannot be overwritten or erased.

Ha intentado copiar una configuración en el banco que el IBM 2216 utiliza actualmente.

Error: File copy failed.

Esta condición se produce cuando falla la operación de copia debido a otra causa distinta a copiar en la configuración activa. La causa más común es especificar las mismas configuraciones de origen y de destino. Cuando se listan (consulte la sección "List" en la página 57) las configuraciones, aparece CORRUPT junto al banco que está dañado.

Describe

Utilice el mandato **describe** para visualizar información acerca de una imagen almacenada.

Sintaxis: describe

Ejemplo: Boot config>**describe**

BANK A				BANK B			
Product ID -	2216-MAS			Product ID -	2216-MAS		
Version	3	Release	2	Version	3	Release	2
Mod	0	PTF	0	Mod	0	PTF	0
Feat.	2822	RPQ	0	Feat.	2822	RPQ	0
Date	31 Dec	1996		Date	31 Dec	1996	

Disable

Utilice el mandato **disable** para desactivar diversas funciones de la gestión de cambios.

Sintaxis:

```
disable                auto-boot
                        fast-boot
```

auto-boot

La inhabilitación del arranque automático provoca que la secuencia de arranque de los dispositivos se detenga en la interfaz de recuperación de servicio, sin ejecutar el código operativo del dispositivo. La modalidad de arranque automático por omisión es “habilitado”.

Ejemplo:

```
Boot config>disable auto-boot
Auto-boot mode is now disabled
```

fast-boot

La inhabilitación del arranque rápido provoca que el dispositivo ejecute pruebas de diagnóstico cuando arranca durante una operación de encendido o de volver a cargar el software. Esto proporciona una mejor detección de los errores de hardware pero provoca tiempos de arranque más lentos. Es la modalidad por omisión y es aconsejable cuando el dispositivo está en un entorno de producción.

Enable

Utilice el mandato **enable** para activar diversas funciones de la gestión de cambios.

Sintaxis:

```
enable                auto-boot
                        fast-boot
```

auto-boot

La habilitación del arranque automático provoca que el dispositivo arranque el código operativo sin detenerse en la interfaz de recuperación de servicio. La modalidad de arranque automático por omisión es “habilitado”

Nota: Para habilitar la modalidad de arranque automático utilizando este mandato, también debe seleccionar la modalidad autónoma en el firmware.

fast-boot

La habilitación del arranque rápido provoca que el dispositivo se salte las pruebas de diagnóstico cuando arranca durante una operación de

encendido o de volver a cargar el software. Esto reduce la detección de errores de hardware pero provoca tiempos de arranque más rápidos. La modalidad por omisión es "inhabilitado", que se recomienda siempre que el dispositivo esté en un entorno de producción.

Ejemplo:

```
Boot config>enable fast-boot
Fast-boot mode is now enabled
```

Erase

Utilice el mandato **erase** para borrar una imagen almacenada o un archivo de configuración.

Sintaxis:

```
erase configuration [archivo]
load [imagen]
```

config o load

Borra un archivo de configuración o una imagen de carga. Entre el número de configuración que se ha de borrar después del mandato **erase**.

Ejemplo: Boot config>erase load

```
+----- BankA -----+----- Description -----+----- Date -----+
| IMAGE - CORRUPT      |                               | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL     | test config for pubs        | 01 Jan 1970 01:26 |
| CONFIG 2 - AVAIL *   | test config for pubs        | 01 Jan 1970 01:13 |
| CONFIG 3 - NONE      |                               | 01 Jan 1970 00:58 |
| CONFIG 4 - AVAIL     |                               | 01 Jan 1970 00:39 |
+----- BankB -----+----- Description -----+----- Date -----+
| IMAGE - ACTIVE       |                               | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL     | test config for pubs        | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL     |                               | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL     |                               | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE *  |                               | 01 Jan 1970 00:24 |
+-----+-----+-----+
* - Last Used Config      L - Config File is Locked
```

```
Select the bank to erase: (A, B): [A] a
Erase SW load image from bank A.
```

Operation completed successfully.

Boot config>list

```
+----- BankA -----+----- Description -----+----- Date -----+
| IMAGE - NONE         |                               | 01 Jan 1970       |
| CONFIG 1 - AVAIL     | test config for pubs        | 01 Jan 1970 00:26 |
| CONFIG 2 - AVAIL *   | test config for pubs        | 01 Jan 1970 01:13 |
| CONFIG 3 - AVAIL     |                               | 01 Jan 1970 00:58 |
| CONFIG 4 - AVAIL     |                               | 01 Jan 1970 00:39 |
+----- BankB -----+----- Description -----+----- Date -----+
| IMAGE - ACTIVE       |                               | 01 Jan 1970       |
| CONFIG 1 - AVAIL     | test config for pubs        | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL     |                               | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL     |                               | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE *  |                               | 01 Jan 1970 00:24 |
+-----+-----+-----+
* - Last Used Config      L - Config File is Locked
```

Auto-boot mode is enabled. Fast-boot mode is disabled.

Ejemplo: Boot config>erase configuration

```
+----- BankA -----+----- Description -----+----- Date -----+
| IMAGE - NONE         |                               | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL     | test config for pubs        | 01 Jan 1970 00:26 |
```

```

| CONFIG 2 - AVAIL * | test config for pubs | 01 Jan 1970 01:13 |
| CONFIG 3 - AVAIL | | 01 Jan 1970 01:26 |
| CONFIG 4 - AVAIL | | 01 Jan 1970 01:39 |
+----- BankB -----+----- Description -----+----- Date -----+
| IMAGE - ACTIVE | | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL | test config for pubs | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL | | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL | | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE * | | 01 Jan 1970 00:24 |
+-----+-----+-----+
* - Last Used Config      L - Config File is Locked

```

Select the source bank: (A, B): [A]
Select the configuration to erase: (1, 2, 3, 4): [1] 3
Erase SW configuration file from bank A, configuration 3.

Operation completed successfully.

```

Boot config>list
+----- BankA -----+----- Description -----+----- Date -----+
| IMAGE - NONE | | 01 Jan 1970 00:14 |
| CONFIG 1 - AVAIL | test config for pubs | 01 Jan 1970 01:13 |
| CONFIG 2 - AVAIL * | test config for pubs | 01 Jan 1970 00:58 |
| CONFIG 3 - NONE | | 01 Jan 1970 00:26 |
| CONFIG 4 - AVAIL | | |
+----- BankB -----+----- Description -----+----- Date -----+
| IMAGE - ACTIVE | | 01 Jan 1970 |
| CONFIG 1 - AVAIL | test config for pubs | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL | | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL | | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE * | | 01 Jan 1970 00:24 |
+-----+-----+-----+
* - Last Used Config      L - Config File is Locked

```

Auto-boot mode is enabled. Fast-boot mode is disabled.

Observe que el mandato list visualiza **NONE** para el banco A, config 3.

Si falla el borrado, aparece un mensaje que indica la anomalía en la consola con los bancos que han fallado.

List

Utilice el mandato **list** para visualizar información acerca de qué imágenes de carga y archivos de configuración están disponibles y activos. También puede utilizar este mandato para visualizar las opciones de arranque y la información de carga planificada.

Sintaxis:

list

Ejemplo: Boot config>list

```

+----- BankA -----+----- Description -----+----- Date -----+
| IMAGE - AVAIL | | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL | test config for pubs | 01 Jan 1970 01:26 |
| CONFIG 2 - AVAIL * | test config for pubs | 01 Jan 1970 01:13 |
| CONFIG 3 - NONE | | 01 Jan 1970 00:58 |
| CONFIG 4 - AVAIL | | 01 Jan 1970 00:39 |
+----- BankB -----+----- Description -----+----- Date -----+
| IMAGE - ACTIVE | | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL | test config for pubs | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL | | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL | | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE * | | 01 Jan 1970 00:24 |
+-----+-----+-----+
* - Last Used Config      L - Config File is Locked
Auto-boot mode is enabled. Fast-boot mode is disabled.

```

Time Activated Load Schedule Information...
 The device is scheduled to reload as follows.
 Date: June 26, 1997
 Time: 16:30
 The load modules are in bank A.
 The configuration is CONFIG 1 in bank A.
 Boot config>

Los posibles descriptores de estado de archivo son:

ACTIVE

Actualmente, el archivo está cargado y en ejecución en el 2216

AVAIL Se trata de un archivo válido que puede activarse (ACTIVE).

CORRUPT

El archivo se ha dañado o no se ha cargado completamente en el 2216.
 Debe sustituirse el archivo.

LOCAL

El archivo sólo se utilizará en la siguiente operación de volver a cargar o de restablecimiento. Después de utilizar el archivo, se colocará en estado AVAIL.

PENDING

Este archivo se cargará en la siguiente operación de volver a cargar, restablecimiento o de encendido del 2216.

Lock

Utilice el mandato **lock** para impedir que el dispositivo grabe una configuración encima de la configuración seleccionada.

Sintaxis:

lock

Ejemplo: Boot config>**lock**

BankA	Description	Date
IMAGE - NONE		01 Jan 1970 01:03
CONFIG 1 - AVAIL	test config for pubs	01 Jan 1970 00:26
CONFIG 2 - AVAIL *	test config for pubs	01 Jan 1970 01:13
CONFIG 3 - NONE		01 Jan 1970 00:58
CONFIG 4 - AVAIL		01 Jan 1970 00:26
BankB	Description	Date
IMAGE - ACTIVE		01 Jan 1970 00:01
CONFIG 1 - AVAIL	test config for pubs	01 Jan 1970 00:54
CONFIG 2 - AVAIL		01 Jan 1970 00:01
CONFIG 3 - AVAIL		01 Jan 1970 00:14
CONFIG 4 - ACTIVE *		01 Jan 1970 00:24

* - Last Used Config L - Config File is Locked

Auto-boot mode is enabled. Select the source bank: (A, B): [A]

Select the source configuration: (1, 2, 3, 4): [1] 4
 Attempting to lock bank A and configuration 4.

Operation completed successfully.

Boot config>**list**

BankA	Description	Date
IMAGE - NONE		01 Jan 1970
CONFIG 1 - AVAIL	test config for pubs	01 Jan 1970 00:13
CONFIG 2 - AVAIL *	test config for pubs	01 Jan 1970 01:13

```

| CONFIG 3 - NONE | | 01 Jan 1970 00:58 |
| CONFIG 4 - AVAIL L | | 01 Jan 1970 00:26 |
+----- BankB -----+----- Description -----+----- Date -----+
| IMAGE - ACTIVE | | |
| CONFIG 1 - AVAIL | test config for pubs | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL | | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL | | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE * | | 01 Jan 1970 00:24 |
+-----+-----+-----+
* - Last Used Config L - Config File is Locked

Auto-boot mode is enabled. Fast-boot mode is disabled.

```

Nota: Observe que el banco A config 4 está marcado con una “L.”

Set

Utilice el mandato **set** para seleccionar el banco de códigos, la configuración que se ha de utilizar y la duración del uso. Las duraciones válidas son:

once La configuración sólo se activa para el próximo arranque.

always

La configuración se activa para todos los arranque subsiguientes hasta que se vuelva a cambiar.

Sintaxis:

set

Ejemplo: Boot config>set

```

+----- BankA -----+----- Description -----+----- Date -----+
| IMAGE - NONE | | 01 Jan 1970 01:03 |
| CONFIG 1 - AVAIL | test config for pubs | 01 Jan 1970 00:13 |
| CONFIG 2 - AVAIL * | test config for pubs | 01 Jan 1970 01:13 |
| CONFIG 3 - NONE | | 01 Jan 1970 00:58 |
| CONFIG 4 - AVAIL | | 01 Jan 1970 00:26 |
+----- BankB -----+----- Description -----+----- Date -----+
| IMAGE - ACTIVE | | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL | test config for pubs | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL | | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL | | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE * | | 01 Jan 1970 00:24 |
+-----+-----+-----+
* - Last Used Config L - Config File is Locked

```

Select the source bank: (A, B): [A] b

Select the source configuration: (1, 2, 3, 4): [1] 4

Select the duration to use for booting: (once, always): [always]

Set SW to boot using bank B and configuration 4, always.

Operation completed successfully.

Boot config>list

```

+----- BankA -----+----- Description -----+----- Date -----+
| IMAGE - NONE | | 01 Jan 1970 |
| CONFIG 1 - AVAIL | test config for pubs | 01 Jan 1970 00:13 |
| CONFIG 2 - AVAIL * | test config for pubs | 01 Jan 1970 01:13 |
| CONFIG 3 - NONE | | 01 Jan 1970 00:58 |
| CONFIG 4 - AVAIL | | 01 Jan 1970 00:26 |
+----- BankB -----+----- Description -----+----- Date -----+
| IMAGE - ACTIVE | | 01 Jan 1970 |
| CONFIG 1 - AVAIL | test config for pubs | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL | | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL | | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE * | | 01 Jan 1970 00:24 |
+-----+-----+-----+

```

* - Last Used Config L - Config File is Locked
 Auto-boot mode is enabled. Fast-boot mode is disabled.

TFTP

Utilice el mandato **tftp** para iniciar las transferencias de archivos TFTP entre el 2216 y los servidores remotos.

Nota: Cuando ejecute unzip en una imagen, verá múltiples archivos que finalizan en ".ld". Utilice el mandato **tftp get load modules** para obtener múltiples módulos de carga.

Sintaxis:

```
tftp get                                    config
                                          load modules

tftp put                                   config
                                          load single imagen
                                          load modules
```

Ejemplo: Boot config>tftp get load single

BankA	Description	Date
IMAGE - NONE		01 Jan 1970 01:03
CONFIG 1 - AVAIL	test config for pubs	01 Jan 1970 00:01
CONFIG 2 - AVAIL *	test config for pubs	01 Jan 1970 01:13
CONFIG 3 - NONE		01 Jan 1970 00:58
CONFIG 4 - AVAIL		01 Jan 1970 00:14
BankB	Description	Date
IMAGE - ACTIVE		01 Jan 1970 00:01
CONFIG 1 - AVAIL	test config for pubs	01 Jan 1970 00:54
CONFIG 2 - AVAIL		01 Jan 1970 00:01
CONFIG 3 - AVAIL		01 Jan 1970 00:14
CONFIG 4 - ACTIVE *		01 Jan 1970 00:24

* - Last Used Config L - Config File is Locked

```
Specify the server IP address (dotted decimal): : [1.2.3.4] 192.9.200.1
Specify the remote file name: : (/u/bin) /usr/2216load/c200-rtr.img
Select the destination bank: (A, B): [A] a
TFTP SW load image
get: /usr/2216load/c200-rtr.img
from: 192.9.200.1
to: bank A.
```

Operation completed successfully.

Nota para la carga dinámica de software: Se recuperarán todos los módulos de carga del directorio especificado como parte de la carga que va al banco. En las cargas para releases anteriores a la Versión 1, Release 2, será un solo módulo de carga. En las cargas de la Versión 1, Release 2 y posteriores, pueden ser varios módulos de carga.

Ejemplo: Boot config>tftp get load modules

BankA	Description	Date
IMAGE - NONE		01 Jan 1970 01:03
CONFIG 1 - AVAIL	test config for pubs	01 Jan 1970 00:01
CONFIG 2 - AVAIL *	test config for pubs	01 Jan 1970 01:13
CONFIG 3 - NONE		01 Jan 1970 00:58
CONFIG 4 - AVAIL		01 Jan 1970 00:14

```

+----- BankB -----+----- Description -----+----- Date -----+
| IMAGE - ACTIVE          |                               | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs         | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                               | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL       |                               | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE *    |                               | 01 Jan 1970 00:24 |
+-----+-----+-----+
* - Last Used Config      L - Config File is Locked

```

```

Specify the server IP address (dotted decimal): : [1.2.3.4] 192.9.200.1
Specify the remote modules directory: : (/u/bin) /usr/22161load/
Select the destination bank: (A, B): [A] a
TFTP SW load image
get: /usr/22161load/LML.1d
from: 192.9.200.1
to: bank A.

```

Operation completed successfully.

Notas:

Cuando ponga archivos en un servidor:

1. Asegúrese de que los archivos del servidor de destino tienen los permisos adecuados que permiten que cualquier usuario grave en ellos. Si no, la operación de poner fallará.
2. Debe tener en cuenta los archivos que pone en el servidor. Para determinar si la imagen del banco es un solo módulo o múltiples módulos, utilice el mandato **describe**. Una carga anterior a la Versión 1, Release 2 es un solo módulo. Las cargas en la Versión 1, Release 2 o posterior son múltiples módulos.

Timedload

Utilice el mandato **timedload** para planificar una carga en un dispositivo, cancelar una carga planificada o ver información de carga planificada.

Este mandato le permite cargar un dispositivo fuera de las horas punta de tráfico en la red, cuando es posible que el personal de soporte no se halle presente.

Nota: También puede utilizar el Programa de configuración para planificar una operación de volver a cargar para un dispositivo, que no se vea afectado por operaciones de volver a cargar ni cortes de alimentación. Normalmente, estas circunstancias harían que se perdiese la operación de volver a cargar. Consulte el capítulo "Utilización del programa de configuración" de la publicación *Guía del usuario del Programa de Configuración para productos Nways Multiprotocol y Access Services* para ver los detalles.

Sintaxis:

```

timedload                activate
                           deactivate
                           view

```

activate

Planifica una carga en el dispositivo. Se le solicitará información de una carga activada a una hora similar a los mandatos **tftp get load** y **tftp get config**. Consulte la sección "TFTP" en la página 60 para obtener información acerca de los parámetros.

Time of day to load the router

Especifica la fecha y la hora en que se ha de cargar el dispositivo. Especifique el valor como AAAAMMDDHHMM, donde:

AAAA es el año de cuatro dígitos

Nota: Si el mes actual del dispositivo es diciembre, los datos del año deben ser del año actual o del año siguiente. De lo contrario, si el mes actual del dispositivo es de enero a noviembre, los datos del año deben ser del año actual.

MM es el mes de dos dígitos.

Valores válidos de MM: De 01 a 12, siendo 01 enero.

DD es el día de dos dígitos del mes.

Valores válidos de DD: De 01 a 31, dependiendo del valor de MM.

HH es la hora de dos dígitos, en formato de 24 horas.

Valores válidos de HH: De 00 a 23

MM es el minuto de dos dígitos de la hora.

Valores válidos de MM: De 00 a 59

Los ejemplos siguientes son de la planificación de una carga desde diversos orígenes.

Ejemplo 1. El origen de los módulos y la configuración de la carga es un sistema principal remoto:

Boot config>timedload activate

BankA	Description	Date
IMAGE - AVAIL		01 Jan 1970 00:01
CONFIG 1 - AVAIL	test config for pubs	01 Jan 1970 01:26
CONFIG 2 - AVAIL *	test config for pubs	01 Jan 1970 01:13
CONFIG 3 - NONE		01 Jan 1970 00:58
CONFIG 4 - AVAIL		01 Jan 1970 00:39
BankB	Description	Date
IMAGE - ACTIVE		01 Jan 1970 00:01
CONFIG 1 - AVAIL	test config for pubs	01 Jan 1970 00:54
CONFIG 2 - AVAIL		01 Jan 1970 00:01
CONFIG 3 - AVAIL		01 Jan 1970 00:14
CONFIG 4 - ACTIVE *		01 Jan 1970 00:24

* - Last Used Config L - Config File is Locked

Time Activated Load Processing...

Select the bank to use: (A, B): [A] a

Do you want to put load modules into the bank? (Yes, No, Quit): [Yes] yes

Do you want to retrieve a SINGLE image or a set of MODULES? [MODULES]? modules

Specify the server IP address (dotted decimal): : [1.2.3.4] 192.9.200.1

Specify the remote modules directory: : (/u/bin) /usr/601bin/205img

The destination bank is bank A

TFTP SW load image

get: /usr/601bin/205img/

from: 192.9.200.1

to: bank A.

tftp: connect to '192.9.200.1'

Operation completed successfully.

Do you want to put a configuration into the bank? (Yes, No, Quit): [Yes] yes

Specify the server IP address (dotted decimal): : [1.2.3.4] 192.9.200.1

Specify the remote file name: : (config.dat) /tftpboot/192.9.200.6.config

The destination bank is bank A

Select the destination configuration: (1, 2, 3, 4): [1] 1

TFTP SW configuration file

```

get: /tftpboot/192.9.200.6.config
from: 192.9.200.1
to: bank A, configuration 1.
tftp: connect to '192.9.200.1'

```

Operation completed successfully.

```

Time of day to load the router (YYYYMMDDHHMM) []? 199706261630
The load timer has been activated.
Boot config>

```

Ejemplo 2. El origen de los módulos y la configuración de la carga es un banco:

```
Boot config>timedload activate
```

BankA	Description	Date
IMAGE - AVAIL		01 Jan 1970 00:01
CONFIG 1 - AVAIL	test config for pubs	01 Jan 1970 01:26
CONFIG 2 - AVAIL *	test config for pubs	01 Jan 1970 01:13
CONFIG 3 - NONE		01 Jan 1970 00:58
CONFIG 4 - AVAIL		01 Jan 1970 00:39
BankB	Description	Date
IMAGE - ACTIVE		01 Jan 1970 00:01
CONFIG 1 - AVAIL	test config for pubs	01 Jan 1970 00:54
CONFIG 2 - AVAIL		01 Jan 1970 00:01
CONFIG 3 - AVAIL		01 Jan 1970 00:14
CONFIG 4 - ACTIVE *		01 Jan 1970 00:24

```

* - Last Used Config      L - Config File is Locked

```

Time Activated Load Processing...

Select the bank to use: (A, B): [A] a

Do you want to put load modules into the bank? (Yes, No, Quit): [Yes] no

Do you want to put a configuration into the bank? (Yes, No, Quit): [Yes] no

Select the configuration to use: (1, 2, 3, 4): [1] 1

Time of day to load the router (YYYYMMDDHHMM) []? 199706261630

The load timer has been activated.

Boot config>

deactivate

Cancela una carga planificada.

Ejemplo 1: Desactivar la carga activada para una hora

```

Boot config>timedload deactivate
Deactivate Load Timer Processing...

```

Do you want to deactivate the load timer? (Yes, No, Quit): [No] yes

The load timer has been deactivated.

Boot config>

view

Visualiza la información de carga planificada.

```

Boot Config> timedload view
Time Activated Load Schedule Information...

```

The router is scheduled to reload as follows.

Date: June 26, 1997

Time: 16:30

The load modules are in bank A.

The configuration is CONFIG 1 in bank A.

Boot config>

Unlock

Utilice el mandato **unlock** para permitir que el dispositivo grave encima de la configuración seleccionada que antes estaba bloqueada.

Sintaxis:

unlock

Ejemplo: Boot config>unlock

```

+----- BankA -----+----- Description -----+----- Date -----+
| IMAGE - NONE                |                               | 01 Jan 1970 01:03 |
| CONFIG 1 - AVAIL            | test config for pubs         | 01 Jan 1970 00:13 |
| CONFIG 2 - AVAIL *          | test config for pubs         | 01 Jan 1970 01:13 |
| CONFIG 3 - NONE             |                               | 01 Jan 1970 00:58 |
| CONFIG 4 - AVAIL L         |                               | 01 Jan 1970 00:26 |
+----- BankB -----+----- Description -----+----- Date -----+
| IMAGE - ACTIVE              |                               | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL            | test config for pubs         | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL            |                               | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL            |                               | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE *         |                               | 01 Jan 1970 00:24 |
+-----+-----+-----+
* - Last Used Config      L - Config File is Locked

```

Select the source bank: (A, B): [A]

Select the source configuration: (1, 2, 3, 4): [1] 4
Attempting to unlock bank A and configuration 4.

Operation completed successfully.

Boot config>list

```

+----- BankA -----+----- Description -----+----- Date -----+
| IMAGE - NONE                |                               | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL            | test config for pubs         | 01 Jan 1970 01:13 |
| CONFIG 2 - AVAIL *          | test config for pubs         | 01 Jan 1970 00:58 |
| CONFIG 3 - NONE             |                               | 01 Jan 1970 00:14 |
| CONFIG 4 - AVAIL            |                               | 01 Jan 1970 00:14 |
+----- BankB -----+----- Description -----+----- Date -----+
| IMAGE - ACTIVE              |                               | 01 Jan 1970       |
| CONFIG 1 - AVAIL            | test config for pubs         | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL            |                               | 01 Jan 1970 00:01 |
| CONFIG 3 - AVAIL            |                               | 01 Jan 1970 00:14 |
| CONFIG 4 - ACTIVE *         |                               | 01 Jan 1970 00:24 |
+-----+-----+-----+
* - Last Used Config      L - Config File is Locked

```

Auto-boot mode is enabled. Fast-boot mode is disabled.

Nota: Observe que el Banco A config 4 ya no está marcado con una “L.”

Update-firmware

Utilice el mandato **update-firmware** para instalar el módulo de carga Firm.Id que ha recibido en el Banco A o en el Banco B del 2216.

No se producirá un arranque automático después de que se ejecute este mandato. Debe establecer el banco desde el que desea rearmar utilizando el mandato Boot config> set y se actualizará el nuevo firmware cuando rearmar. Consulte la sección “Capítulo 3. Acceso al firmware desde la interfaz de línea de mandatos” en la página 31 para obtener información de rearmar.

Sintaxis:

update-firmware

Ejemplo:

Boot config>update

```

+-----+-----+
|          BANK A          |          BANK B          |
| Product ID - 2216-MAS    | Product ID - 2216-MAS    |
| Version 3 Release 1     | Version 3 Release 1     |
| Mod 0 PTF 0             | Mod 0 PTF 0             |
| Feat. 2807 RPQ 0        | Feat. 2807 RPQ 0        |
| Date 14 Jul 1998 07:45  | Date 7 Aug 1998 14:05   |
| Build cc_155b           | Build cc_158b           |
+-----+-----+

```

```
| | test-load |  
+-----+-----+
```

DO NOT POWER OFF while firmware is updating.
To exit, type Ctrl-c at the Select bank/restore prompt.

Select the source bank or P to restore from Precover.img: (A, B, P): [A]B

```
Using Local Firmware image /hd0/sys1/Firm.ld  
flash: ID = 0x01A4, sector wp = 0x00  
flash: Found /hd0/sys1/Firm.ld:524774 bytes.  
flash: Loading file /hd0/sys1/Firm.ld...  
flash: File /hd0/sys1/Firm.ld loaded at 0x0025f0ec for 524288 bytes  
flash: Creating /hd0/precover.img from flash  
flash: Recovery image created.  
flash: Validating firmware image  
flash: Update from:0025F0EC, offset=00010000, flash size=524288  
flash: Erasing sector 7f  
flash: Erasing sector 3f  
flash: Erasing sector 1f  
flash: Erasing sector f  
flash: Erasing sector 7  
flash: Erasing sector 3  
flash: Erasing sector 1  
flash: Current addr = 0007f000
```

Operation completed successfully.

Capítulo 7. El proceso CONFIG (CONFIG - Talk 6) y sus mandatos

Este capítulo describe los mandatos de configuración y operativos del proceso CONFIG. Incluye las secciones siguientes:

- “¿Qué es CONFIG?”
- “Entrada y salida de CONFIG” en la página 76
- “Mandatos CONFIG” en la página 76

¿Qué es CONFIG?

El proceso de Configuración (CONFIG) es un proceso de segundo nivel de la interfaz de usuario del dispositivo. Mediante la utilización de los mandatos CONFIG, puede:

- Establecer o cambiar diversos parámetros de configuración
- Añadir o suprimir una interfaz en la configuración del hardware
- Entrar en la modalidad de mandatos Boot CONFIG
- Entrar en la modalidad de Configuración rápida
- Borrar, listar, o actualizar la información de configuración
- Habilitar o inhabilitar el inicio de sesión de consola
- Comunicarse con los procesos del tercer nivel, incluyendo los entornos de protocolo

Nota: Consulte el capítulo “Migrating to a New Code Level” de la publicación *2216 Nways Multiaccess Connector Service and Maintenance Manual* para obtener información sobre la migración a un nuevo nivel de código.

CONFIG le permite visualizar o cambiar la información de configuración almacenada en la memoria de configuración no volátil del dispositivo. Los cambios en los parámetros del sistema y de protocolo no surten efecto hasta que se vuelve a cargar el software de dispositivo. (Para obtener más información, consulte el mandato **reload** de OPCON en “¿Qué es el proceso OPCON?” en la página 33).

Nota: Debe entrar el mandato **write** para guardar los cambios en la memoria instantánea del dispositivo.

La interfaz de mandatos CONFIG está compuesta de niveles que se llaman modalidades. Cada modalidad tiene su propio indicador. Por ejemplo, el indicador para el protocolo SNMP es `SNMP config>`.

Si desea saber el proceso y la modalidad con la que se está comunicando, pulse **Intro** para visualizar el indicador. Algunos mandatos de este capítulo como, por ejemplo, los mandatos **network** y **protocol**, le permiten acceder a varios niveles de CONFIG y acceder a ellos. Consulte la Tabla 7 en la página 76 para ver una lista de los mandatos que puede emitir desde el proceso CONFIG.

Modalidad de Sólo configuración

Se entra en la modalidad de Sólo configuración si el archivo de configuración que está utilizando está vacío o no hay ningún protocolo configurado. También se puede entrar manualmente en la modalidad de Sólo configuración para la recuperación de una configuración no válida que provoca que el direccionador falle durante el arranque.

Utilización del proceso CONFIG

Entrada automática en la modalidad de Sólo configuración

Se entra en la modalidad de Sólo configuración si el direccionador se arranca con un archivo de configuración vacío o el archivo de configuración contiene datos de configuración incompletos.

Las condiciones siguientes provocan que el direccionador entre en modalidad de Sólo configuración:

- Los dispositivos están configurados pero no hay ningún protocolo configurado.
- En caso de supresión de toda la información de la interfaz del direccionador.
- El archivo de configuración está vacío.

Entrada manual en la modalidad de Sólo configuración

Para entrar en la modalidad de Sólo configuración, realice una de las acciones siguientes:

- Vuelva a cargar el direccionador sin ninguna configuración.

Para volver a cargar el direccionador sin ninguna configuración, utilice el mandato de configuración de la gestión de cambios **erase**. Después utilice el mandato de configuración de la gestión de cambios **set** para seleccionar el archivo de configuración vacío. Puede acceder a los mandatos de configuración de la gestión de cambios desde el indicador `Boot>`.

- Vuelva a cargar el direccionador sin ninguna interfaz configurada.
- Vuelva a cargar el direccionador sin ningún protocolo configurado.

Para crear una configuración que no tenga ningún protocolo configurado, utilice el mandato **clear** para borrar la información de configuración de los protocolo.

Nota: Si está habilitado el arranque automático y pulsa **Control-C** mientras se carga el software, pasará directamente al supervisor de rutina de carga `>` sin ver el texto y puede saltarse el paso 1. De lo contrario, aparece el texto siguiente:

```
PROM Load/Dump Program * Revision: 1.15 *
Copyright IBM Corp. 1994, 1997
Host **VL-51* loading
Using Ethernet at ( 81600, 94).
Trying host 128.185.210.125, via 128.185.123.28
      file loads/latest-gen.rbx2-multisna.ldc
.loading
.....
....
```

1. Si falta información de arranque, el software se cargará desde el IBD. Si el primer archivo IBD no es válido como, por ejemplo, una archivo de configuración, el software irá al indicador de carga manual:

```
No valid boot records found, attempting IBD load
Loading using IBD Load Image "v12-15.cfg"
Bad record header 0

No valid server configured -- Entering manual mode
Device types available:
```

```
IBD
Token Ring
WAN
```

Device type:

2. Pulse **Control-C** para ir al supervisor de rutina de carga. Aparece el indicador `>`.
3. Boot to Config-Only mode.

```
>bc
```

```
PROM Load/Dump Program * Revision: 1.15 *
Copyright IBM Corp. 1994, 1997
Host **VL-51* loading

Device types available:
```

```

IBD
Ethernet
WAN

Device type [Ethernet]:
Connector Type (AUI/RJ45) [AUTO_CONFIG]:
Interface IP address [128.185.123.51]: 10.1.155.22
IP mask [FFFFFF00]:
Boot from host [128.185.210.125]:
Via gateway [128.185.123.28]: 43
Boot file name [loads/latest-gen.rbx2-multisna.ldc]:

Using Ethernet at ( 0, 0).
Trying host 128.185.210.125, via 128.185.123.28
file loads/latest-gen.rbx2-multisna.ldc
.loading
*.....
Starting at 1040010

The Standalone Configuration Process. You are here because
The watchdog timer timed out and/or Autoboot not selected

Config (only)>

```

De lo contrario, el direccionador se rearrancará. Si falta la información de arranque, el software se cargará desde la unidad de disco duro.

Consulte la sección “Capítulo 3. Acceso al firmware desde la interfaz de línea de mandatos” en la página 31 para obtener más información.

Configuración rápida

La Configuración rápida (Quick Config) proporciona un conjunto mínimo de mandatos que le permiten configurar protocolos de puente y de direccionamiento presentes en la carga del dispositivo. También puede configurar una comunidad SNMP con acceso WRITE_READ_TRAP. Esto es útil durante la configuración inicial porque el programa de configuración utiliza los mandatos SNMP SET para transferir la configuración.

Importante: Como mínimo debe haberse configurado un dispositivo de red antes de utilizar la configuración rápida. Para añadir un dispositivo, utilice el mandato **add device** en el indicador `config(only)>` o `config>`. Consulte la sección “Acceso al proceso de configuración de interfaces de red” en la página 16 para obtener más información.

La tabla siguiente lista los protocolos soportados por la Configuración rápida.

Tabla 6. Posibilidades de la Configuración rápida

Protocolos ATM	Protocolos de puente	Protocolos de direccionamiento
Emulación LAN	STB, SRT, SRB	IP, IPX, DNA IV

La Configuración rápida complementa el proceso de configuración existente ofreciendo un método abreviado. Este método abreviado le permite configurar el número mínimo de parámetros para estos protocolos de puente y protocolos de direccionamiento sin tener que salir y entrar en los distintos procesos de configuración. Los demás parámetros se establecen en los valores por omisión seleccionados.

Las situaciones que llaman la configuración rápida del dispositivo son:

- La memoria de configuración está en blanco o dañada como, por ejemplo, cuando se produce una de las situaciones siguientes:
 - Se configura el dispositivo por primera vez.

Utilización del proceso CONFIG

- Las fluctuaciones de voltaje han dañado el disco fijo.
- Por motivos de demostración, para los cuales es necesario configurar rápidamente el dispositivo para demostrar sus posibilidades.
- En las pruebas de referencia, para que empiecen las pruebas sin tener que conocer los mandatos del sistema operativo del dispositivo.

La configuración rápida funciona de la siguiente manera:

- Pregunta una serie de cuestiones con valores por omisión.
- Ofrece un método abreviado a la configuración detallada del conjunto de mandatos de la modalidad normal.

La modalidad de Configuración rápida establece unos parámetros por omisión basándose en las respuestas a las preguntas de la configuración. Lo que no se puede configurar con la Configuración rápida puede configurarlo utilizando la Configuración después de salir de la Configuración rápida.

No puede suprimir la información de Configuración rápida desde la Configuración rápida. Sin embargo, puede corregir la información saliendo y volviendo a la Configuración rápida o entrando el mandato **reload** como respuesta a las preguntas de la Configuración rápida.

Para obtener información completa sobre la utilización del software de Configuración rápida, consulte el “Apéndice A. Consulta para la configuración rápida” en la página 809.

Entrada manual en la modalidad de Configuración rápida

Puede que desee ejecutar manualmente la Configuración rápida para demostrar las posibilidades del dispositivo o para efectuar una reconfiguración dinámica para realizar pruebas de referencia sin tener que aprender los mandatos del sistema operativo del dispositivo.

Para entrar en la Configuración rápida, escriba **qconfig** en el indicador `Config>`.

Salida de la modalidad de Configuración rápida

Para salir de la Configuración rápida, reinicie entrando **r** en cualquier indicador. Siga las consultas hasta que entre **no** y después, entre **q** para abandonar. El direccionador vuelve al indicador `Config (only)>` o `Config>`.

Configuración del acceso de usuario

El proceso de configuración de dispositivos permite un máximo de 50 nombres de usuarios, contraseñas y niveles de permisos. Cada usuario necesita tener asignada una contraseña y un nivel de permiso. Hay tres niveles de permiso: *Administración*, *Operación* y *Supervisión*.

Para obtener más información, consulte la página en la página 83.

Acceso de soporte técnico

Si es el administrador del sistema, la primera vez que añade un nuevo usuario, se le pregunta si desea añadir el acceso de Soporte técnico. Si responde sí, se otorga al Soporte técnico los mismos privilegios que tiene como administrador del sistema.

La contraseña para esta cuenta la selecciona automáticamente el software y la conoce el servicio técnico. Esta contraseña puede cambiarse utilizando el mandato **change user**; sin embargo, si la cambia, el servicio al cliente no podrá proporcionarle soporte remoto. Para obtener información adicional sobre el uso del mandato **change user**, consulte la sección “Change” en la página 84.

Configuración de interfaces de repuesto

Ocasionalmente, puede necesitar configurar una nueva interfaz junto con sus protocolos de puente y de direccionamiento sin tener que reiniciar el dispositivo. Puede conseguirlo configurando unas cuantas **interfaces de repuesto** en el dispositivo. Las interfaces de repuesto son útiles si:

- Está “conectando en caliente” un nuevo adaptador en el dispositivo.
Puede instalar el adaptador, configurarlo y, después, activarlo, sin desenchufar o reiniciar el dispositivo.
- Está añadiendo circuitos de marcación en el dispositivo.
Utilice las interfaces de repuesto para añadir nuevos circuitos de marcación V.25bis o RDSI en una interfaz V.25bis o RDSI existente.

Nota: No puede añadir interfaces de repuesto a interfaces RDSI T1/E1 canalizadas.

- Está añadiendo clientes ATM LAN Emulation.
Utilice las interfaces de repuesto para añadir clientes ATM LAN Emulation Ethernet o de Red en Anillo a una interfaz ATM existente.
- Está añadiendo redes virtuales a un Adaptador de canal ESCON o a un Adaptador de canal paralelo existente.

Para configurar una interfaz de repuesto:

1. Acceda al proceso CONFIG entrando **configuration**.
2. Configure el número de interfaces de repuesto para el dispositivo utilizando el mandato **set spare-interfaces**.
3. Salga del proceso CONFIG pulsando **Control-P**.
4. Vuelva a cargar el dispositivo.

Ejemplo:

```
* configuration
Config> set spare 2
Config>
* reload
Are you sure you want to reload the gateway? (Yes or [No]) yes
```

Cuando el dispositivo se vuelve a cargar, las interfaces de repuesto se instalan como dispositivos nulos.

Para utilizar una de las interfaces de repuesto:

1. Inserte el nuevo adaptador en la ranura del adaptador.

Nota: Si utiliza un adaptador de canal ESCON o Paralelo, tiene la posibilidad de definir interfaces de repuesto para cada una de las redes conectadas sin utilizar adaptadores adicionales. En este caso, puede saltarse este paso.

2. Acceda al proceso CONFIG entrando **configuration**.
3. Añada una interfaz o un circuito de marcación utilizando el mandato **add device**, si es necesario.
4. Configure la interfaz de repuesto utilizando el mandato **net** para configurar la interfaz o añadir clientes de ATM LAN Emulation.
5. Configure los diversos protocolos y características utilizando los mandatos **protocol** y **feature**.
6. Salga del proceso CONFIG pulsando **Control-P**.
7. Acceda al proceso GWCON entrando **console**.

Utilización del proceso CONFIG

8. Ponga en línea la nueva interfaz en la red utilizando el mandato **activate**.

El ejemplo siguiente muestra cómo configurar y activar un nuevo circuito de marcación en el cual el protocolo IP esté habilitado. No aparece la configuración del circuito de marcación ni del protocolo IP.

Ejemplo:

```
* configuration
Config> add device dial-circuit
Config> net 6
Circuit configuration
Circuit config>

:
Aquí configuraría el circuito de marcación

:

Circuit config> exit
Config> protocol ip
IP>

:
Aquí configuraría el protocolo IP en el circuito de marcación.

:

IP> exit
Config>
*console
+ activate 6
```

El ejemplo siguiente muestra cómo configurar y activar un nuevo ATM LAN Emulation Client en el cual está configurado el protocolo IP. Las configuraciones de IP y de ATM LAN Emulation Client no aparecen.

```
* configuration
Config> net 0
ATM User Configuration
ATM Config> le-client
ATM LAN Emulation Clients Configuration
LE Client config> add token-ring
Added Emulated LAN as interface 6
LE Client config> config 6
ATM LAN Emulation Client configuration
:
:
(Aquí configuraría el ATM LAN Emulation Client)
:

Token Ring Forum Compliant LEC Config> exit
LE Client config> exit
ATM Config> exit
Config> protocol ip
IP Config>

:

(Aquí configuraría IP en el ATM LAN Emulation Client)
:

IP Config> exit
Config> write
control-p
* console
+ activate 6
Interface 6 activated successfully
```

Restricciones para las interfaces de repuesto

El mandato **activate** no puede utilizarse para activar una nueva interfaz en la red bajo las condiciones siguientes:

Utilización del proceso CONFIG

- Si ya ha entrado un mandato **delete interface**. El dispositivo debe reiniciarse si no se ha suprimido **ninguna** interfaz. No puede suprimir una interfaz de repuesto (indicada por **null** en las pantallas de listas).
- Si la interfaz de repuesto es la única interfaz que habilita un protocolo o característica. El protocolo o característica ya debe estar habilitado en una interfaz existente para que una interfaz de repuesto pueda utilizarlo.
- Si la nueva interfaz de repuesto tiene un tamaño de cabecera o de cola mayor que los tamaños para otras interfaces.
- Si no hay suficiente memoria para asignar los almacenamientos intermedios de recepción para la nueva interfaz.

En estos casos, debe reiniciar el dispositivo para poner en línea la nueva interfaz.

El mandato **activate** no activa todas las interfaces de repuesto. Para determinar cómo afecta el mandato **activate** a las interfaces de repuesto, consulte la sección relativa a la reconfiguración dinámica que se incluye en los capítulos de configuración y supervisión de cada interfaz

Un par de interfaces de repuesto no incluyen información de reconfiguración dinámica en sus descripciones y no pueden activarse en la red utilizando el mandato **activate**. Estas interfaces se incluyen en la lista siguiente:

- SDLC
- V.25bis

Debe reiniciar el dispositivo para poner en línea estas interfaces.

Puede configurar el protocolo siguiente en las interfaces de repuesto, pero no puede activarlo en la red utilizando el mandato **activate**:

- OSI/DECnet V

Nota: Cuando utilice el programa de configuración, utilice lo siguiente para trabajar con interfaces de repuesto:

1. Realice los cambios de configuración para la interfaz de repuesto en el dispositivo
2. Entre el mandato **activate** en el dispositivo para poner en línea la interfaz de repuesto, los protocolos y las características
3. Recupere la configuración utilizando el programa de configuración
4. Guarde la configuración recuperada en la base de datos del programa de configuración

Ciertas funciones tienen requisitos para el mandato **activate**. Los requisitos de la mayoría de las funciones afectadas se describen en los capítulos relativos a la configuración y la supervisión de cada función. En el capítulo aplicable, consulte la sección sobre la reconfiguración dinámica.

Para las funciones que no se describen en los capítulos relativos a la configuración y la supervisión, los requisitos del mandato **activate** son:

DECnet IV Para activar este protocolo en una interfaz de repuesto, primero debe activar la interfaz y, después, configurar el protocolo en la interfaz activada. Utilice el mandato **set** de DECnet IV para activar los cambios en la configuración.

Utilización del proceso CONFIG

Restablecimiento de interfaces

Ocasionalmente, puede necesitar cambiar la configuración de una interfaz de red junto con sus protocolos de puente y direccionamiento sin reiniciar el dispositivo. El mandato **reset** le permite inhabilitar una interfaz de red y, después, habilitarla utilizando nuevos parámetros de configuración de interfaz, puente y direccionamiento.

Los parámetros de configuración de la interfaz, los protocolos y las características se cambian utilizando los mandatos del proceso CONFIG (talk 6). Los mandatos de talk 6 afectan al contenido de la memoria de configuración. Los cambios en la configuración se activan emitiendo el mandato **reset** del proceso GWCON (talk 5).

Para restablecer una interfaz:

1. Acceda al proceso CONFIG (talk 6).
2. Utilice el mandato **net** y otros mandatos para cambiar los parámetros de configuración.
3. Utilice los mandatos **protocol** y **feature** para cambiar los parámetros de configuración basados en la interfaz.
4. Salga del proceso CONFIG pulsando **Control-P**.
5. Acceda al proceso GWCON (talk 5).
6. Utilice el mandato **reset** para restablecer la interfaz y los protocolos y características de la interfaz.

Ejemplo:

```
* configuration
Config>net 1
PPP Config>

. . . change PPP parameters . . .

PPP Config>exit
Config>protocol ipx
IPX Config>

. . . change IPX parameters on the PPP interface . . .

IPX Config>exit
Config>
*talk 5
+reset 1
Resetting net 1 PPP/0...successful
```

Nota: Cuando utilice el programa de configuración, efectúe lo siguiente para realizar cambios en la configuración de interfaces existentes:

1. Efectúe los cambios de configuración para la interfaz en el dispositivo
2. Entre el mandato **reset** para restablecer los parámetros de interfaz, protocolo y características
3. Recupere la configuración utilizando el programa de configuración
4. Guarde la configuración recuperada en la base de datos del programa de configuración

Restricciones para restablecer interfaces

No puede utilizarse el mandato **reset** para restablecer una interfaz de red si:

- Ya ha entrado un mandato **delete interface**. Debe volver a cargar el dispositivo si ha suprimido alguna interfaz.
- Ha cambiado el hardware o el tipo de enlace de datos. Por ejemplo, se ha cambiado el tipo de enlace de datos de PPP a Frame Relay.

- Ha configurado una MTU mayor.
- Ha configurado un protocolo de direccionamiento o un puente en la interfaz, pero el protocolo de direccionamiento o el puente no está activo actualmente en el dispositivo.

En estas situaciones, debe volver a cargar el dispositivo para activar los cambios de configuración.

Los cambios configurados para ciertas interfaces, características y protocolos no se pueden activar utilizando el mandato **reset**. El uso del mandato **reset** para la mayoría de estas interfaces, características y protocolos se describe en la sección relativa a la reconfiguración dinámica del capítulo de configuración y supervisión.

La interfaz V.25bis no puede activarse utilizando el mandato **reset** y el mandato **reset** para esta interfaz no se describe en el capítulo de configuración y supervisión.

Debe volver a cargar el dispositivo para activar los cambios de configuración.

La lista siguiente incluye los protocolos y las características que no pueden activarse utilizando el mandato **reset** y para los cuales no se describe el mandato **reset** en el capítulo de configuración y supervisión.

- AppleTalk
- Vines
- OSI/DECnet V

También existen requisitos asociados a **reset** para determinadas funciones que no se describen en los capítulos de configuración y supervisión. Estos requisitos se listan por función en la tabla siguiente:

Compresión	La compresión necesita tamaños grandes de cabecera y de cola. A menos que la compresión ya esté habilitada en alguna otra interfaz, es probable que los tamaños de cabecera y de cola sean demasiado pequeños. En este caso, la compresión se inhabilita automáticamente en la interfaz y se anota cronológicamente un mensaje ELS (en lugar de hacer que falle toda el restablecimiento de la interfaz).
------------	---

DNA IV	Utilice el mandato set de DNA IV para activar los cambios de configuración.
--------	--

Utilización de vuelcos del sistema

Una herramienta útil para depurar los problemas del 2216 es el vuelco del sistema. El vuelco es una instantánea comprimida que el sistema guarda en la unidad de disco duro, si está presente, o en un sistema principal remoto de la red .

Para configurar el vuelco:

1. Especifique los tres archivos de vuelco que guardará. Consulte la página 108 para obtener más información.
2. Especifique si desea que se vuelva a habilitar el vuelco después de que produzca un vuelco. Consulte la página 107 para obtener más información.
3. Habilite el vuelco en el 2216. Consulte la página 95 para obtener más información.

Utilización del proceso CONFIG

Puede ver el estado de los vuelcos del sistema o recuperar un vuelco del sistema. Consulte las secciones “System View” en la página 113 y “Recuperación del sistema” en la página 112, respectivamente.

Entrada y salida de CONFIG

Para entrar en el proceso CONFIG desde OPCON y obtener el indicador CONFIG, entre el mandato **configuration**. Alternativamente, puede entrar el mandato **talk** de OPCON y el PID para CONFIG. El PID para CONFIG es 6.

* **configuration**

o

* **talk 6**

La consola visualiza el indicador CONFIG (Config>). Si no aparece el indicador, pulse la tecla **Intro** de nuevo.

Para salir de CONFIG y volver al indicador OPCON (*), entre el carácter de interceptación. (El valor por omisión es **Control-P**.)

Mandatos CONFIG

Esta sección describe los mandatos CONFIG. Cada mandato incluye una descripción, los requisitos de su sintaxis y un ejemplo. Los mandatos CONFIG se resumen en la Tabla 7.

Después de acceder al entorno CONFIG, entre los mandatos de configuración en el indicador Config>.

Tabla 7. Resumen de los mandatos CONFIG

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página 10.
Add	Añade una interfaz a la configuración del dispositivo o un usuario al dispositivo.
Boot	Entra en la modalidad de mandatos Boot CONFIG.
Change	Cambia la contraseña de un usuario o los valores de los parámetros de un usuario asociados a esta interfaz. También cambia una ranura/puerto de una interfaz.
Clear	Borra la información de configuración.
Delete	Suprime una interfaz de la configuración del direccionador o suprime un usuario configurado. También suprime archivos de vuelco del sistema.
Disable	Inhabilita la finalización de mandatos, el inicio de sesión desde una consola remota, inhabilita el uso del módem
Enable	Habilita la finalización de mandatos, inicio de sesión desde una consola remota habilita el uso del módem
Event	Entra en el entorno de configuración del Sistema de anotación cronológica de sucesos.
Feature	Proporciona acceso a los mandatos de configuración para características de dispositivo independientes, fuera de los procesos normales de configuración de protocolos y de interfaces de red.
List	Visualiza los parámetros del sistema, la configuración del hardware, una lista completa de usuarios.
Load	Lista, añade o suprime paquetes de software opcionales.
Network	Entra en el entorno de configuración de la red especificada.

Tabla 7. Resumen de los mandatos CONFIG (continuación)

Mandato	Función
Patch	Modifica la configuración global del dispositivo.
Performance	Proporciona una instantánea de las estadísticas de utilización del procesador principal.
Protocol	Entra en el entorno de mandatos del protocolo especificado.
Qconfig	Inicia el proceso de Configuración rápida.
Set	Establece los parámetros en todo el sistema para los almacenamientos intermedios, el nombre de sistema principal, el temporizador de inactividad, el tamaño de paquete, el nivel del indicador, el número de interfaces de repuesto, los parámetros de vuelco, la ubicación y la persona de contacto.
System Retreive	Recupera vuelcos
System View	Visualiza los valores de vuelco y el estado actual del vuelco. También visualiza un resumen de los vuelcos.
Time	Busca la hora del sistema y la visualiza en la consola.
Unpatch	Restaura las variables de parche en los valores por omisión.
Update	Actualiza la memoria de configuración cuando reciba una nueva carga de software.
Write	Graba la información de la configuración actual en memoria no volátil.

Add

Utilice el mandato **add** para añadir una interfaz a la configuración o al acceso de usuario. Este mandato también vuelve a crear registros de dispositivo si se pierde la configuración inadvertidamente.

Sintaxis:

```
add                callback . . .
                   device
                   isdn-address . . .
                   ppp-user
                   tunnel-profile
                   user . . .
                   v25-bis-address
```

callback

Utilice el mandato **add callback** para añadir, suprimir o listar información para la llamada de retorno de RDSI.

Add Añade un número de llamada de retorno a las listas de autenticación.

Delete Suprime un número de llamada de retorno de la lista de autenticación.

Lists Visualiza la lista de autenticación y otra información relacionada.

device *tipo_dispositivo información-configuración-adicional*

Con el mandato **add device**, debe entrar el tipo de dispositivo de interfaz (*tipo_dispositivo*). Se le solicitan parámetros de configuración adicionales. Esta información adicional varía según el dispositivo y la plataforma.

Mandatos CONFIG

Consulte la sección “Adición de dispositivos” en la página 16 para obtener información adicional acerca del tipo de dispositivo y los parámetros de configuración.

Nota: Si está añadiendo más de una interfaz, es importante el orden en el que las añade ya que el dispositivo asigna un número secuencial de interfaz al dispositivo cuando se añade. Este número de interfaz es un número de índice de la lista de dispositivos; enlaza el dispositivo con la información de configuración restante como, por ejemplo, las direcciones IP asociadas con el dispositivo. (Para obtener más información, consulte el mandato **list devices**, “List” en la página 97.)

Toda la información de configuración de dispositivos y protocolos relacionada con las interfaces de red se almacena por número de interfaz. Cualquier cambio realizado en los números de interfaz invalidará una gran parte de la información de configuración de dispositivos de los protocolos.

Ejemplo:

```
add device atm
Device Slot #(1-8) [1]? 2
Adding CHARM ATM Adapter device in slot 2 port 1 as interface x
(donde x es el número de interfaz asignado)
```

Para determinar los dispositivos que puede añadir, utilice el mandato **add devices ?**.

isdn-address *nombre-dirección dirección-marcación-red dirección-submarcación-red*
Añade los números locales y remotos de los puntos finales RDSI que se comunicarán con el direccionador.

nombre-dirección

Puede ser cualquier cosa (como una descripción del puerto)

dirección-marcación-red

El número de teléfono del puerto local o de destino.

dirección-submarcación-red

La parte adicional del número de teléfono como, por ejemplo, una extensión, que se interpreta cuando la interfaz se conecta a un PBX; este parámetro es opcional.

Nota: Puede utilizar signos de puntuación como, por ejemplo, paréntesis y guiones, pero no son significativos (el direccionador sólo utiliza los números).

```
Ejemplo: add isdn-address line 1 local
Assign network dial address [0 - 32 digits]? 1 2345 67
Assign network subdial address [0 - 19 digits]? 98765
```

ppp-user

Añade el perfil de usuario de un usuario remoto a la base de datos de usuarios PPP local. Puede añadir un máximo de 500 usuarios. Se añade un usuario PPP para cada direccionador remoto o cliente DIALs que puede conectarse al dispositivo que está configurando. Debe configurar usuarios PPP si existe alguna de las condiciones siguientes:

- Está utilizando protocolos de autenticación PPP, el cifrado PPP o permite que los usuarios utilicen la característica de marcación externa. Necesita configurar un usuario PPP para el tipo de cifrado - Encryption Control Protocol (ECP) o Microsoft Point-to-Point Encryption (MPPE); sin embargo, MPPE no necesita clave de cifrado.

- Desea que la base de datos de usuarios PPP se almacene localmente y la gestione el dispositivo. Si desea que la información de usuario PPP se obtenga de un servidor RADIUS, TACACS o TACACS+, debe configurar la característica de Autenticación en lugar de configurar usuarios PPP locales.

Nota: MPPE no puede utilizar los servidores RADIUS, TACACS ni TACACS+. Para MPPE, la base de datos de usuarios PPP debe ser local.

Si se ha habilitado ECP para el usuario, se le solicita el nombre de usuario PPP, la contraseña, la dirección IP y la clave de cifrado.

Si la característica DIALs está en la carga de software, se le pide si se trata de un usuario DIALs.

Si está añadiendo un usuario para un cliente DIALs, se le solicita el nombre de sistema principal, el tipo de ruta, la máscara de red, el tiempo de conexión y la información de llamada de retorno.

Consulte la sección “Utilización de un servidor Acceso de marcación de entrada a las LAN (DIALs)” de la publicación *Utilización y configuración de las características* para obtener más información.

Un perfil de usuario almacenado localmente en el dispositivo consta de los elementos siguientes:

Name El id de usuario del usuario PPP, utilizado durante la autenticación. Consulte la sección “Protocolos de autenticación de PPP” en la página 628.

Password

La contraseña que el usuario y el dispositivo reconocen, utilizada durante la autenticación. Puede tener hasta 31 caracteres de longitud, consta de cualquier carácter alfanumérico y es sensible a las mayúsculas y minúsculas. Consulte la sección “Protocolos de autenticación de PPP” en la página 628 para obtener más información.

Enter again to verify

Vuelva a entrar la contraseña para la verificación.

Allow inbound access

Permite el acceso de entrada para ese perfil de usuario.

Valores válidos: yes, no

Valor por omisión: no

Will user be tunneled?

Especifica si este usuario de marcación de entrada debe llegar por túnel a un destino LNS. Si entra “yes”, se le solicita información acerca del LNS.

Valores válidos: yes, no

Valor por omisión: no

Number of days before account expiry

El número de días para que caduque la cuenta.

Valores válidos: De 0 a 360

Mandatos CONFIG

Valor por omisión: 180

Number of grace logins allowed

El número de intentos de inicio de sesión permitidos después de que caduque la contraseña.

Valores válidos: De 0 a 100

Valor por omisión: 0

Hostname to use when connecting to this peer:

Especifica el nombre de sistema principal local de este LAC que se pasa como identificación al LNS durante la configuración del túnel.

Tunnel Server endpoint:

Especifica la dirección IP del LNS al que este usuario llega por túnel.

Type of Route

Es "Ruta de sistema principal" o "Ruta de red."

Generalmente, se aplica una ruta de sistema principal para el acceso de un solo usuario. Normalmente, se aplica una ruta de red a un acceso de red. Una ruta de red permite entrar una máscara de red.

IP Address

Dirección IP que se ha de asignar a un usuario.

Una dirección IP basada en el perfil de un usuario para ofrecer a un cliente de marcación de entrada, si la pide. Hay varias maneras de que un 2216 obtenga una dirección IP para un cliente de marcación de entrada. Consulte la sección "IP Control Protocol" en la página 634 para obtener más información.

Valores válidos: Cualquier dirección IP válida

Valor por omisión: ninguna

Net-Route Mask

Máscara para un usuario de la red.

Si el usuario de marcación de entrada se está conectando a una interfaz PPP habilitada por DIAL, el direccionador añade automáticamente una ruta estática temporal para ese cliente para la duración de la sesión PPP. Normalmente, esta ruta estática tiene la máscara de red 255.255.255.255 (el valor por omisión), que implica que sólo hay un sistema principal IP en el otro extremo del enlace PPP. Sin embargo, se puede alterar temporalmente la máscara de red. Si está configurada, esta máscara se utiliza al añadir la ruta temporal. Un ejemplo es un direccionador pequeño con una sola red de sistemas principales que llama a un direccionador habilitado por DIAL. La única ruta para el pequeño direccionador de oficina se instalará automáticamente basándose en el perfil de usuario, haciendo que no sea necesario configurar protocolos de direccionamiento entre los dos sistemas principales y reduciendo la actividad general del tráfico de direccionamiento a través de un enlace potencialmente lento.

Hostname

El nombre de sistema principal que se ha de enviar al servidor Proxy DHCP para que Dynamic DNS lo utilice. Consulte la sección "Utilización de un servidor Acceso de marcación de entrada a las

LAN (DIALs)” de la publicación *Utilización y configuración de las características* para obtener más información.

Time-Allotted

El tiempo que un usuario DIAL puede estar conectado. Se trata del total para esta sesión y no debe confundirse con un temporizador de inactividad.

Valores válidos: De 0 a 71 827 788 minutos (0=sin límite)

Valor por omisión: 0

Callback type

Método de llamada de retorno, “Voluntaria” o “Necesaria.” Los parámetros de llamada de retorno se utilizan para especificar si el direccionador volverá a llamar al usuario y a qué número. Consulte la sección “Configuración de llamada de retorno PPP” en la página 631 para obtener información adicional.

Set encryption key

Especifica si se ha de habilitar el cifrado ECP para este usuario/puerto.

Valores válidos: yes, no

Valor por omisión: no

ECP encryption key

Entre la clave de cifrado ECP de 16 caracteres.

Este parámetro sólo se visualiza si se ha habilitado PPP Encryption Control Protocolo (ECP) utilizando el mandato de talk 6 PPP Config> **enable ecp**. MPPE no necesita ninguna clave de cifrado. Esta clave de cifrado ECP la utiliza PPP Encryption Control Protocolo (ECP). Consulte la sección “Utilización y configuración de protocolos de encriptación” de la publicación *Utilización y configuración de las características*.

Disable user

Le permite inhabilitar un perfil de usuario.

Valores válidos: yes, no

Valor por omisión: no

Ejemplo:

```
Config>add ppp-user
Enter name: [ ]? pppusr01
Password:
Enter again to verify:
Allow inbound access for user? (Yes, No): [yes]
Will user be tunneled? (Yes, No): [No]
Number of days before account expiry[0-1000] [0]? 10
Number of grace logins allowed after an expiry[0-100] [0]? 5
IP address: [0.0.0.0]? 1.1.1.1
Set ECP encryption key for this user? (Yes, No): [No] no
Disable user ? (Yes, No): [No]

      PPP user name: pppusr01
      User IP address: 1.1.1.1
      Virtual Conn: disabled
      Encryption: disabled
      Status: enabled
      Login Attempts: 0
      Login Failures: 0
      Lockout Attempts: 0
      Account expires: Sun 17Feb2036 06:28:16
      Account duration: 10 days 00.00.00
```

Mandatos CONFIG

```
    Password Expiry: <unlimited>
User 'pppusr01' has been added
```

Ejemplo:

```
Config>add ppp-user
Enter name: [ ]? tunusr01
Password:
Enter again to verify:
Allow inbound access for user? (Yes, No): [yes]
Will user be tunneled? (Yes, No): [No] yes
Enter hostname to use when connection to this peer: []? host01
Tunnel-Server endpoint address: [0.0.0.0]? 1.1.1.1

--more--          PPP user name: tunusr01
--more--          Endpoint: 1.1.1.1
--more--          Hostname: host01

User 'tunusr01' has been added
```

Ejemplo con cifrado ECP:

```
Config>add ppp-user
Enter name: [ ]? ppp_user2
Password:
Enter again to verify:
Allow inbound access for user? (Yes, No): [Yes]
Will user be tunneled? (Yes, No): [No]
Is this a 'DIALS' user? (Yes, No): [Yes]
Type of route? (hostroute, netroute): [hostroute]
Number of days before account expiry[0-1000] [0]?
Number of grace logins allowed after an expiry[0-100] [0]?
IP address: [11.0.0.185]?
Allow virtual connections? (Yes, No): [No]
Give user default time allotted ? (Yes, No): [Yes]
Enable callback for user? (Yes, No): [No]
Will user be able to dial-out ? (Yes, No): [No]
Set ECP encryption key for this user? (Yes, No): [No] y
Encryption key should be 16 characters long.
Encryption Key (16 characters ) in Hex(0-9, a-f, A-F):
Encryption Key again (16 characters) in Hex(0-9, a-f, A-F):
ECP encryption key is set.
Disable user ? (Yes, No): [No]

    PPP user name: ppp_user2
    User IP address: 11.0.0.185
    Netroute Mask: 255.255.255.255
    Hostname:          Virtual Conn: disabled
    Time allotted: Box Default
    Callback type: disabled
    Dial-out: disabled
    Encryption: enabled
    Status: enabled
    Login Attempts: 0
    Login Failures: 0
    Lockout Attempts: 0
    Account Expiry: Password Expiry:
Is information correct? (Yes, No, Quit): [Yes]

User 'ppp_user1' has been added
```

tunnel *nombre-tunnel*

Proporciona un acceso de similar de túnel a través de una red IP para el direccionador. Entonces se autoriza al similar a iniciar las sesiones PPP con túnel en el direccionador. Para configurar un túnel debe especificar:

Name El nombre del sistema principal del similar de túnel.

Hostname to use when connecting to this peer

El nombre de sistema principal local que se ha de utilizar cuando se conecta a este similar. Este nombre se utiliza para la identificación del sistema principal en el similar.

Set shared secret

Especifica si se ha de utilizar un secreto compartido.

Shared Secret

El secreto compartido entre LAC y LNS. Debe ser exactamente el mismo en ambos extremos del túnel.

Enter again to verify

Entre de nuevo el secreto compartido para verificación.

Tunnel-Server endpoint address

La dirección IP del similar de túnel (LAC o LNS).

Ejemplo:

```
Config> add tunnel
Enter name: []? tunnel02
Enter hostname to use when connecting to this peer: []? host02
Set shared secret? (Yes, No): [No]? yes
Shared secret for tunnel authentication:
Enter again to verify:
Tunnel-Server endpoint address: [0.0.0.0]? 2.2.2.22
```

```
Tunnel name: tunnel02
Endpoint: 2.2.2.22
```

user nombre_usuario

Proporciona a un usuario el acceso al dispositivo. Puede autorizar hasta 50 usuarios a acceder al dispositivo. Cada *nombre_usuario* tiene ocho caracteres y es sensible a las mayúsculas y minúsculas.

Cuando se añade el primer usuario, se habilita automáticamente el inicio de sesión de consola. Debe asignarse uno de los niveles de permiso definidos en la Tabla 8 a cada usuario que se añade.

Cuando añada usuarios, establezca la autenticación de inicio de sesión en local. De lo contrario, debe utilizar un servidor remoto.

Tabla 8. Permiso de acceso

Nivel de permiso	Descripción
Administrador (A)	Visualiza la información de configuración y de usuario, añade/modifica/suprime la información de configuración y de usuario. El Administrador puede acceder a cualquier función del direccionador.
Operador (O)	Visualiza la configuración del direccionador, visualiza las estadísticas, ejecuta pruebas que pueden provocar interrupciones, cambia dinámicamente el funcionamiento del direccionador y reinicia el direccionador. Los operadores no pueden modificar la configuración permanente del direccionador. Se pueden deshacer todas las acciones con un reinicio del sistema.
Supervisor (M)	Visualiza la configuración del direccionador y las estadísticas pero no puede modificar ni interrumpir el funcionamiento del direccionador.
Soporte técnico	Permite que el servicio técnico obtenga acceso al direccionador si se ha olvidado la contraseña. No se puede asignar a los usuarios.

Nota: Para añadir un usuario, debe tener permiso de administración. No se ha de reinicializar el direccionador después de añadir un usuario.

Ejemplo:

Mandatos CONFIG

```
add user Juan
Enter password:
Enter password again:
Enter permission (A)admin, (O)perations, (M)onitor [A]?
Do you want to add Technical Support access? (Yes or [No]):
```

Enter password

Especifica la contraseña de acceso para el usuario. Está limitada a 80 caracteres alfanuméricos y es sensible a las mayúsculas y minúsculas.

Enter password again

Confirma la contraseña de acceso para el usuario.

Enter permission

Especifica el nivel de permiso para el usuario: A, O o M (consulte la Tabla 8 en la página 83).

v25-bis-address

Añade los números locales y remotos de los puntos finales V.25bis que se comunican con el direccionador. El *nombre-dirección* de red puede ser cualquier cosa como, por ejemplo, una descripción del puerto. Puede utilizar cualquier serie de un máximo de 23 caracteres ASCII imprimibles. La *dirección-marcación-red* es el número de teléfono del puerto local o de destino. Para obtener más información, consulte la página “Capítulo 50. Utilización de la interfaz de red V.25bis” en la página 751.

Nota: Puede utilizar signos de puntuación como, por ejemplo, paréntesis y guiones, pero no son significativos (el direccionador sólo utiliza los números).

Ejemplo: add v25-bis-address
remote-site baltimore 1-909-555-0983

Boot

Utilice el mandato **boot** para entrar en el entorno de mandatos Boot CONFIG. Para obtener información sobre Boot CONFIG, consulte la sección “Capítulo 5. Utilización de BOOT Config para efectuar la gestión de cambios” en la página 47.

Sintaxis:

boot

Change

Utilice el mandato **change** para modificar una interfaz de la configuración, cambiar su propia contraseña o cambiar la información de usuario.

Sintaxis:

```
change                device . . .
                        password
                        ppp_user . . .
                        tunnel-profile
```

device *tipo_dispositivo*

Con el mandato **change device** puede:

- Cambiar la ranura de una interfaz existente. (Cambiar la ranura x del registro de interfaz n por y cuando la ranura y está desocupada.)

Mandatos CONFIG

- Cambiar el puerto de una interfaz existente. (Cambiar el puerto x del registro de interfaz n por y cuando el puerto y está desocupado.)
- Intercambiar ranuras de dos interfaces existentes. (Intercambiar la ranura x y la ranura y en los registros de la interfaz por x ó y.)
- Intercambiar puertos de dos interfaces existentes. (Intercambiar el puerto u y la ranura x de un registro de interfaz por el puerto v y la ranura y de otro registro de interfaz del mismo tipo de hardware.)
- Sustituir la ranura de una interfaz existente por la ranura de otra. (La configuración de interfaz de la ranura x se convertirá en la configuración de interfaz para la ranura y. Los registros de interfaz para la ranura y se suprimirán.)
- Sustituir el puerto de una interfaz existente por el puerto de otra. (La configuración de interfaz para la ranura x puerto u se convertirá en la configuración de interfaz para la ranura y puerto v. El registro de interfaz para la ranura y puerto v se suprimirá.)

Cuando la ranura de destino está ocupada:

1. Si selecciona la opción de “intercambio”, se intercambian las ranuras de origen y de destino de todos los registros de la interfaz en los que aparecen.
2. Si selecciona la opción de “sustitución”, la configuración de interfaz para la ranura x se convertirá en la configuración de interfaz para la ranura y. Los registros de interfaz para la ranura y se suprimirán.

Cuando el puerto de destino está ocupado:

1. Si selecciona la opción de “intercambio”, se pueden intercambiar los puertos de origen y de destino en sus registros respectivos de interfaz si sus tipos de hardware de esos registros de interfaz son idénticos. Por ejemplo, RDSI T1/J1 de 1 puerto.
2. Si selecciona la opción de “sustitución”, la configuración de interfaz para la ranura x puerto u se convierte en la configuración de interfaz para la ranura y puerto v. El registro de interfaz para la ranura y puerto v se suprime.

Nota: Una tarjeta adaptadora Ethernet o de Red en Anillo necesita dos ranuras vacías si está instalada en las ranuras 3, 4, 7 u 8. Por lo tanto, sólo se puede instalar un adaptador de Red en Anillo o Ethernet en las ranuras 3 ó 4 (o en las ranuras 7 u 8) si las dos ranuras 3 y 4 (o 7 y 8) están desocupadas.

Si intenta cambiar la ranura de un adaptador de Red en Anillo o Ethernet por las ranuras 3 ó 4 (o 7 u 8) cuando tanto 3 como 4 (o 7 y 8) están desocupadas, no se acepta el cambio y se emite un mensaje de aviso tal como se muestra en el ejemplo “Cambiar la ranura 6 de la interfaz 1 por la ranura 8 desocupada” de la página 86.

Ejemplo - Cambiar (sustituir) la ranura 1 de la interfaz 1 por la ranura 2 ocupada:

```
Config>list dev
Ifc 0 CHARM ATM          Slot: 2 Port: 1
Ifc 1 CHARM ATM          Slot: 1 Port: 1

Config>change device
Which configured slot would you like to change? (1, 2) [2]? 1
Which slot would you like to change to? (1-2) [1]? 2

Configuration for slot 2 already exists. You can:
```

Mandatos CONFIG

```
a - abort this operation
r - replace configuration
   (Interface configuration for slot 1 will become interface
   configuration for slot 2. Interface records for slot 2
   will be deleted!)
s - swap configuration (slot 1 will be swapped with slot 2.)
r
```

Moved slot 2 to slot 1 in 1 intf (port) record...

```
Config>list dev
Ifc 0 CHARM ATM                               Slot: 2 Port: 1
```

Ejemplo - Cambiar la ranura 5 de la interfaz 0 por la ranura 7 desocupada:

```
Config>list dev
Ifc 0 Token Ring                             Slot: 5 Port: 1
Ifc 1 Token Ring                             Slot: 6 Port: 1
Ifc 2 Token Ring                             Slot: 1 Port: 1
Ifc 3 8 port EIA-232E/V.24 PPP               Slot: 2 Port: 0
Ifc 4 8 port EIA-232E/V.24 PPP               Slot: 2 Port: 1
Ifc 5 8 port EIA-232E/V.24 PPP               Slot: 2 Port: 2
Ifc 6 6 port V.35/V.36 PPP                   Slot: 3 Port: 0
Ifc 7 6 port V.35/V.36 PPP                   Slot: 3 Port: 5
Ifc 8 8 port EIA-232E/V.24 PPP               Slot: 4 Port: 0
```

```
Config>change device
Which configured slot would you like to change? (1, 2, 3, 4, 5, 6)[1]? 5
Change all ports on slot # 5 (Yes or No)? [Yes]: y
Which slot would you like to change to? (1-8) [1]? 7
```

Changed slot 5 to slot 7 in 1 intf (port) record...

```
Config>list dev
Ifc 0 Token Ring                             Slot: 7 Port: 1
Ifc 1 Token Ring                             Slot: 6 Port: 1
Ifc 2 Token Ring                             Slot: 1 Port: 1
Ifc 3 8 port EIA-232E/V.24 PPP               Slot: 2 Port: 0
Ifc 4 8 port EIA-232E/V.24 PPP               Slot: 2 Port: 1
Ifc 5 8 port EIA-232E/V.24 PPP               Slot: 2 Port: 2
Ifc 6 6 port V.35/V.36 PPP                   Slot: 3 Port: 0
Ifc 7 6 port V.35/V.36 PPP                   Slot: 3 Port: 5
Ifc 8 8 port EIA-232E/V.24 PPP               Slot: 4 Port: 0
```

La interfaz 0 se ha cambiado a la ranura 7.

Ejemplo - Cambiar la ranura 6 de la interfaz 1 por la ranura 8 desocupada:

```
Config>change device
Which configured slot would you like to change? (1, 2, 3, 4, 6, 7)[1]? 6
Change all ports on slot # 6 (Yes or No)? [Yes]: y
Which slot would you like to change to? (1-8) [1]? 8
```

```
Cannot add Token Ring to slot 8.
Slot 7 is occupied so Token Ring cannot be added in slot 8.
```

Nota: Consulte la nota de la página 2 en la página 85 para ver los requisitos para cambiar las ranuras 3, 4, 7 y 8 para Red en Anillo o Ethernet.

Ejemplo - Intercambiar la ranura 6 de la interfaz 1 por la ranura 1 ocupada:

```
Config>change device
Which configured slot would you like to change? (1, 2, 3, 4, 6, 7) [1] 6
Change all ports on slot # 6 (Yes or No)? [Yes]: y
Which slot would you like to change to? (1-8) [1]? 1
```

```
Configuration for slot 1 already exists. You can:
a - abort this operation
r - replace configuration
   (Interface configuration for slot 6 will become interface
   configuration for slot 1. Interface records for slot 1
   will be deleted!)
s - swap configuration (slot 1 will be swapped with slot 6.)
s
```

Swapped slot 6 with slot 1 in 1 port record...

```
Config>list dev
Ifc 0 Token Ring                Slot: 7 Port: 1
Ifc 1 Token Ring                Slot: 1 Port: 1
Ifc 2 Token Ring                Slot: 6 Port: 1
Ifc 3 8 port EIA-232E/V.24 PPP  Slot: 2 Port: 0
Ifc 4 8 port EIA-232E/V.24 PPP  Slot: 2 Port: 1
Ifc 5 8 port EIA-232E/V.24 PPP  Slot: 2 Port: 2
Ifc 6 6 port V.35/V.36 PPP      Slot: 3 Port: 0
Ifc 7 6 port V.35/V.36 PPP      Slot: 3 Port: 5
Ifc 8 8 port EIA-232E/V.24 PPP  Slot: 4 Port: 0
```

Se han intercambiado las configuraciones para la interfaz 2 y la interfaz 1.

Ejemplo - La ranura 1 de la interfaz 1 sustituye a la ranura 6, se suprime la interfaz 1:

```
Config>change device
Which configured slot would you like to change? (1, 2, 3, 4, 6, 7) [1] 6
Change all ports on slot # 6 (Yes or No)? [Yes]: y
Which slot would you like to change to? (1-8) [1]? 1
```

```
Configuration for slot 1 already exists. You can:
a - abort this operation
r - replace configuration
   (Interface configuration for slot 6 will become interface
   configuration for slot 1. Interface records for slot 1
   will be deleted!)
s - swap configuration (slot 1 will be swapped with slot 6.)
r
```

Moved slot 6 to slot 1 in 1 intf (port) record...

```
Config>list dev
Ifc 0 Token Ring                Slot: 7 Port: 1
Ifc 1 Token Ring                Slot: 1 Port: 1
Ifc 2 8 port EIA-232E/V.24 PPP  Slot: 2 Port: 0
Ifc 3 8 port EIA-232E/V.24 PPP  Slot: 2 Port: 1
Ifc 4 8 port EIA-232E/V.24 PPP  Slot: 2 Port: 2
Ifc 5 6 port V.35/V.36 PPP      Slot: 3 Port: 0
Ifc 6 6 port V.35/V.36 PPP      Slot: 3 Port: 5
Ifc 7 8 port EIA-232E/V.24 PPP  Slot: 4 Port: 0
```

El registro de la ranura 6 sustituye al registro de ranura 1 original y se vuelven a numerar las demás interfaces.

Ejemplo - Cambiar la ranura 2 por la ranura 5 desocupada:

```
Config>change device
Which configured slot would you like to change? (1, 2, 3, 4, 7) [1]? 2
Change all ports on slot # 2 (Yes or No)? [Yes]: y
Which slot would you like to change to? (1-8) [1]? 5
```

Changed slot 2 to slot 5 in 3 intf (port) records...

```
Config>list dev
Ifc 0 Token Ring                Slot: 7 Port: 1
Ifc 1 Token Ring                Slot: 1 Port: 1
Ifc 2 8 port EIA-232E/V.24 PPP  Slot: 5 Port: 0
Ifc 3 8 port EIA-232E/V.24 PPP  Slot: 5 Port: 1
Ifc 4 8 port EIA-232E/V.24 PPP  Slot: 5 Port: 2
Ifc 5 6 port V.35/V.36 PPP      Slot: 3 Port: 0
Ifc 6 6 port V.35/V.36 PPP      Slot: 3 Port: 5
Ifc 7 8 port EIA-232E/V.24 PPP  Slot: 4 Port: 0
```

Las interfaces 2, 3 y 4 que se habían configurado previamente en la ranura 2 están configuradas ahora en la ranura 5.

Ejemplo - Cambiar el puerto 1 ranura 5 por el puerto 0 de la ranura 2 desocupada:

```
Config>change device
Which configured slot would you like to change? (1, 3, 4, 5, 7) [1]? 5
Change all ports on slot # 5 (Yes or No)? [Yes]: n
Which port would you like to change in slot 5? (0, 1, 2) [0]? 1
Which slot would you like to change to? (1-8) [1]? 2
Which port would you like port 1 in slot 5 to move to in slot2?#(0-7)[0]? 0
```

Changed slot 5 port 1 to slot 2 port 0...

Mandatos CONFIG

```
Config>list dev
Ifc 0 Token Ring                Slot: 7 Port: 1
Ifc 1 Token Ring                Slot: 1 Port: 1
Ifc 2 8 port EIA-232E/V.24 PPP  Slot: 5 Port: 0
Ifc 3 8 port EIA-232E/V.24 PPP  Slot: 2 Port: 0
Ifc 4 8 port EIA-232E/V.24 PPP  Slot: 5 Port: 2
Ifc 5 6 port V.35/V.36 PPP      Slot: 3 Port: 0
Ifc 6 6 port V.35/V.36 PPP      Slot: 3 Port: 5
Ifc 7 8 port EIA-232E/V.24 PPP  Slot: 4 Port: 0
```

La interfaz 3, que estaba en la ranura 5 - puerto 1, se ha cambiado a la ranura 2 puerto 0.

Ejemplo - Cambiar el puerto 0 ranura 2 por el puerto 5 de la ranura 3 (tipos de hardware diferentes):

```
Config>change device
Which configured slot would you like to change? (1, 2, 3, 4, 5, 7) [1]? 2
Change all ports on slot # 2 (Yes or No)? [Yes]: n
Which port would you like to change in slot 2? (0) [0]? 0
Which slot would you like to change to? (1-8) [1]? 3
Which port would you like port 0 in slot 2 to move to in slot 3? #(0-7) [0] 5
Aborting - source and target slots of different type.
```

Ejemplo - Cambiar el puerto 0 ranura 2 por el puerto 5 de la ranura 4 (el mismo tipo de hardware):

```
Config>change device
Which configured slot would you like to change? (1, 2, 3, 4, 5, 7) [1]? 2
Change all ports on slot # 2 (Yes or No)? [Yes]: n
Which port would you like to change in slot 2? (0) [0]? 0
Which slot would you like to change to? (1-8) [1]? 4
Which port would you like port 0 in slot 2 to move to in slot 4? #(0-7)[0] 5
Changed slot 2 port 0 to slot 4 port 5...
```

```
Config>list dev
Ifc 0 Token Ring                Slot: 7 Port: 1
Ifc 1 Token Ring                Slot: 1 Port: 1
Ifc 2 8 port EIA-232E/V.24 PPP  Slot: 5 Port: 0
Ifc 3 8 port EIA-232E/V.24 PPP  Slot: 4 Port: 5
Ifc 4 8 port EIA-232E/V.24 PPP  Slot: 5 Port: 2
Ifc 5 6 port V.35/V.36 PPP      Slot: 3 Port: 0
Ifc 6 6 port V.35/V.36 PPP      Slot: 3 Port: 5
Ifc 7 8 port EIA-232E/V.24 PPP  Slot: 4 Port: 0
```

La interfaz 3 que estaba en el puerto 0, ranura 2 se cambia por el puerto 5, ranura 4.

Ejemplo - Cambiar el puerto 5 ranura 4 por el puerto 1 ranura 4 (las mismas ranuras):

```
Config>change device
Which configured slot would you like to change? (1, 3, 4, 5, 7) [1]? 4
Change all ports on slot # 4 (Yes or No)? [Yes]: n
Which port would you like to change in slot 4? (0, 5) [0]? 5
Which slot would you like to change to? (1-8) [1]? 4
Which port would you like port 5 in slot 4 to move to in slot 4? #(0-7) [0] 1
Changed slot 4 port 5 to slot 4 port 1...
```

```
Config>list dev
Ifc 0 Token Ring                Slot: 7 Port: 1
Ifc 1 Token Ring                Slot: 1 Port: 1
Ifc 2 8 port EIA-232E/V.24 PPP  Slot: 5 Port: 0
Ifc 3 8 port EIA-232E/V.24 PPP  Slot: 4 Port: 1
Ifc 4 8 port EIA-232E/V.24 PPP  Slot: 5 Port: 2
Ifc 5 6 port V.35/V.36 PPP      Slot: 3 Port: 0
Ifc 6 6 port V.35/V.36 PPP      Slot: 3 Port: 5
Ifc 7 8 port EIA-232E/V.24 PPP  Slot: 4 Port: 0
```

La interfaz 3 está ahora en el puerto 1, ranura 4.

Ejemplo - Cambiar (intercambiar) el puerto 1 ranura 4 por el puerto 0 ocupado de la ranura 5:

```

Config>change device
Which configured slot would you like to change? (1, 3, 4, 5, 7) [1]? 4
Change all ports on slot # 4 (Yes or No)? [Yes]: n
Which port would you like to change in slot 4? (0, 1) [0]? 1
Which slot would you like to change to? (1-8) [1]? 5
Which port would you like port 1 in slot 4 to move to in slot 5? #(0-7) [0] 0

Configuration for slot 5 (port 0) already exists. You can:
a - abort this operation
r - replace configuration
    (Interface record for slot 4 port 1 will become interface
    configuration for slot 5 port 0. The interface record for
    slot 5 port 0 will be deleted!)
s - swap configuration (slot 5 port 0 will be swapped with slot 4
    port 1.)
s

Swapped slot 4 port 1 with slot 5 port 0...

```

```

Config>list dev
Ifc 0 Token Ring                Slot: 7 Port: 1
Ifc 1 Token Ring                Slot: 1 Port: 1
Ifc 2 8 port EIA-232E/V.24 PPP  Slot: 4 Port: 1
Ifc 3 8 port EIA-232E/V.24 PPP  Slot: 5 Port: 0
Ifc 4 8 port EIA-232E/V.24 PPP  Slot: 5 Port: 2
Ifc 5 6 port V.35/V.36 PPP      Slot: 3 Port: 0
Ifc 6 6 port V.35/V.36 PPP      Slot: 3 Port: 5
Ifc 7 8 port EIA-232E/V.24 PPP  Slot: 4 Port: 0

```

La interfaz 2 y la interfaz 3 han intercambiado sus configuraciones de puerto y de ranura.

Ejemplo - Cambiar (sustituir) el puerto 1 ranura 4 por el puerto 0 ocupado de la ranura 5:

```

Config>change device
Which configured slot would you like to change? (1, 3, 4, 5, 7) [1]? 4
Change all ports on slot # 4 (Yes or No)? [Yes]: n
Which port would you like to change in slot 4? (0, 1) [0]? 1
Which slot would you like to change to? (1-8) [1]? 5
Which port would you like port 1 in slot 4 to move to in slot 5? #(0-7) [0] 0

Configuration for slot 5 (port 0) already exists. You can:
a - abort this operation
r - replace configuration
    (Interface configuration for slot 4 port 1 will become interface
    configuration for slot 5 port 0. The interface record for
    slot 5 port 0 will be deleted!)
s - swap configuration (slot 5 port 0 will be swapped with slot 4
    port 1.)
r

Moved slot 4 port 1 to slot 5 port 0...

```

```

Config>list dev
Ifc 0 Token Ring                Slot: 7 Port: 1
Ifc 1 Token Ring                Slot: 1 Port: 1
Ifc 2 8 port EIA-232E/V.24 PPP  Slot: 5 Port: 0
Ifc 3 8 port EIA-232E/V.24 PPP  Slot: 5 Port: 2
Ifc 4 6 port V.35/V.36 PPP      Slot: 3 Port: 0
Ifc 5 6 port V.35/V.36 PPP      Slot: 3 Port: 5
Ifc 6 8 port EIA-232E/V.24 PPP  Slot: 4 Port: 0

```

La interfaz 2 está configurada para la ranura 5 - puerto 0. Se suprime la interfaz 3 original y se vuelven a numerar las otras interfaces.

password

Modifica la contraseña del usuario que ha iniciado la sesión.

Nota: Para cambiar la contraseña de usuario, debe tener permiso de administración.

Ejemplo:

```

change password
Enter current password:
Enter new password:
Enter new password again:

```

Mandatos CONFIG

Enter current password

Especifica la contraseña actual.

Enter new password

Especifica la nueva contraseña.

Enter new password again

Especifica la nueva contraseña otra vez para confirmación. Si la confirmación no coincide con la contraseña nueva anterior, la contraseña vieja continúa en vigor.

ppp_user

Cambia la información para un usuario PPP específico.

Sintaxis:

```
change ppp_user           encryption-key  
                             parameters  
                             password
```

encryption-key

Cambia la clave de cifrado para un usuario PPP. El ejemplo siguiente muestra el diálogo para cambiar una clave de cifrado.

Ejemplo - Cambiar clave de cifrado:

```
Config>change ppp_user encryption-key  
Enter user name: [ ]? leslie  
Enable encryption for this user/port (y/n) [No]:y  
Encryption key should be 16 characters long.  
Encryption Key (16 characters ) in Hex(0-9, a-f, A-F):  
Encryption Key again (16 characters) in Hex(0-9, a-f, A-F):  
User 'leslie' has been updated  
Config>
```

parameters

Cambia todas las opciones de usuario PPP para un usuario. Este parámetro funciona de manera similar a **add ppp_user** excepto en que los valores mostrados entre [] son los valores actuales y el mandato de cambio no verifica los cambios ni los lista de nuevo cuando se finaliza. Consulte la sección "Add" en la página 77 para ver los detalles acerca del mandato **add ppp_user**.

password

Cambia la contraseña para el usuario PPP.

Ejemplo - Cambiar contraseña:

```
Config>change ppp_user password  
Enter user name: [ ]? sam  
Password:  
Enter password again:  
User 'sam' has been updated  
Config>
```

user Modifica la información de usuario que se ha configurado previamente con el mandato **add user**.

Nota: Para cambiar un usuario, debe tener permiso de administración.

Ejemplo:

```
change user  
User name: [ ]  
Change password? (Yes or No)  
Change permission? (Yes or [No])
```

tunnel-profile

Cambia la configuración para un similar de túnel.

```

Config>change tunnel-profile
Enter name: []? lac.org
Enter hostname to use when connecting to this peer: [lns.org]?
set shared secret? (Yes, No): [No]
Tunnel-Server endpoint address: [11.0.0.1]? 11.0.0.2

profile 'lac.org' has been updated
Config>

```

Clear

Utilice el mandato **clear** para suprimir la información de configuración del dispositivo de la memoria de configuración no volátil.

Atención: Utilice este mandato únicamente después de llamar al servicio técnico.

Sintaxis:

```

clear
  all
  ap2 (AppleTalk 2)
  arp (ARP)
  asrt (Adaptive Source Route Protocol)
  appn (Advanced Peer-to-Peer Networking)
  atm (Asynchronous Transfer Mode)
  auth (Authentication)
  bgp (Border Gateway Protocol)
  boot
  brs (Bandwidth Reservation)
  callback
  cmprs (Data Compression)
  dls (Data Link Switching)
  device
  dialer-circuit
  dn (DECnet)
  els (Event Logging System Information)
  fr (Frame Relay)
  gsm (OSI)
  hdlc
  hod (Host On-Demand Client Cache) *
  hostname
  ip (IP)
  ip-security
  ipv6
  ipx (Novell IPX)
  isdn

```

Mandatos CONFIG

l2tp
lnm
mcf
named-profiles
nat
ndp6
ndr
osi (OSI)
ospf (OSPF routing protocol)
ppp (Point-to-Point)
prompt
rip6
rsvp
sdlc
snmp
srly (SDLC Relay)
tcp/ip-host
time (Time of day information)
tsf (Thin Server)
user
v25 bis
vines (Banyan VINES)
webc (Web Server Cache) *
wrs (WAN Restoral feature)
x25
xtp

***Nota:** HOD y WEBC no coexisten en la misma imagen de software.

Para borrar un proceso de la memoria de configuración no volátil, entre el mandato **clear** y el nombre del proceso. Para borrar toda la información de la memoria de configuración, excepto la información del dispositivo, utilice el mandato **clear all**. Para borrar toda la información, incluso la información del dispositivo, utilice el mandato **clear all** y, a continuación, el mandato **clear device**.

El mandato **clear user** borra toda la información de usuario excepto la información de inicio de sesión de la consola de dispositivo. Ésta se deja habilitada (si se ha configurado así) aunque el valor por omisión sea “inhabilitada”.

Notas:

1. Para borrar la información de usuario, debe tener permiso de administración.
2. Hay otros muchos elementos en la lista, dependiendo de lo que se incluya en la carga de software.

Ejemplo: clear els

You are about to clear all Event Logging configuration information
Are you sure you want to do this (Yes or No):

Nota: El mensaje anterior aparece para cualquier configuración de parámetro que esté borrando.

Delete

Utilice el mandato **delete** para eliminar una interfaz o rango de interfaces de la lista de dispositivos almacenados en la configuración o para eliminar un usuario. Para utilizar el mandato **delete**, debe tener el permiso de administración.

Sintaxis:

```
delete                _coprocessor . . .
                       _interface . . .
                       _dump-files
                       _isdn-address
                       _ppp_user . . .
                       _tunnel
                       _user . . .
                       _v25-bis-address
```

interface [*númerointfz* o *rangonúmerointfcs*]

Para suprimir una interfaz, entre el número de interfaz o red como parte del mandato. (Sólo pueden suprimirse los dispositivos que se han añadido con el mandato **add device**.) Para obtener el número de interfaz que el dispositivo asigna, utilice el mandato **list device**.

El mandato de supresión de interfaz suprime la configuración de dispositivo y cualquier otra información de protocolo para esa interfaz. Sin embargo, el dispositivo continuará ejecutando la configuración anterior hasta que se vuelva a cargar.

Si se suprime una interfaz RDSI base o una interfaz ATM base, también se suprimirán todas las interfaces virtuales que se ejecutan en esa red base. Por lo tanto, cualquier circuito de marcación configurado en una interfaz RDSI base se eliminará cuando se suprima la interfaz RDSI. También, al suprimir una red base ATM, se suprimirán todos los clientes LAN Emulation Client que se ejecutan en la interfaz ATM base.

Para suprimir un rango de interfaces, especifique la primera y la última interfaz del rango separadas por un guión, tal como se muestra en el ejemplo siguiente:

```
delete interface 13-21
```

También puede entrar un número de interfaz o rango de números de interfaces cuando se lo solicite.

isdn-address *nombre-dirección*

Elimina todas las direcciones RDSI añadidas previamente.

Mandatos CONFIG

Nota: Si *nombre-dirección* contiene espacios (por ejemplo, **remote site XYZ**), no puede entrar el mandato en una línea. Escriba `delete isdn-address` y pulse **Intro**. Después entre el nombre cuando se lo solicite.

ppp_user *nombre_usuario*

Suprime un usuario de la base de datos de usuarios PPP.

tunnel-profile

Suprime un túnel de la base de datos de perfiles de túneles.

user *nombre_usuario*

Elimina el acceso de usuario al dispositivo para el usuario especificado.

v25-bis-address *nombre-dirección*

Elimina una dirección V25 bis añadida previamente.

Nota: Si *nombre-dirección* contiene espacios (por ejemplo, **remote site Baltimore**), no puede entrar el mandato en una línea. Escriba `delete v25-bis-address` y pulse **Intro**. Después entre el nombre cuando se lo solicite.

Disable

Utilice el mandato **disable** para inhabilitar la finalización de mandatos, el inicio de sesión desde una consola remota, inhabilita el uso del módem

Sintaxis:

disable command-completion
console-login
dump-memory . . .
interface . . .
reboot-system . . .

command-completion

Utilice el mandato **disable command-completion** para inhabilitar la función de finalización automática de mandatos. Consulte la sección “Finalización del mandato” en la página 23 para ver una explicación de la función de finalización automática de mandatos.

Nota: La finalización de mandatos está *inhabilitada* por omisión para las configuraciones existentes y está *habilitada* por omisión para las nuevas configuraciones. Si está utilizando una configuración existente y desea utilizar la finalización de mandatos, necesita utilizar el mandato **enable command-completion** para habilitar esta función.

console-login

Inhabilita la solicitud de un ID de usuario y una contraseña en la consola física. El valor por omisión es inhabilitada.

interface *númerointerfaz*

Hace que se inhabilite la interfaz especificada después de emitir el mandato **reload**. El valor por omisión es habilitado.

dump-memory

Inhabilita el vuelco de la memoria del sistema en el disco duro instalado cuando se produce un error grave.

reboot-system

Inhabilita el re arranque del sistema cuando se produce un error grave. Puede ser aconsejable si el personal de servicio de la red desea resolver problemas en línea. El re arranque del sistema no puede inhabilitarse a menos que también se inhabilite el vuelco de la memoria del sistema. Si intenta inhabilitar el re arranque del sistema mientras el vuelco de la memoria está habilitado, se cancela anormalmente el re arranque del sistema y se visualiza el mensaje siguiente:

```
System reboot not disabled: memory dumping must be disabled first
```

Enable

Utilice el mandato **enable** para habilitar la finalización de mandatos, el inicio de sesión desde una consola remota, inhabilita el uso del módem

Sintaxis:

```
enable                command-completion
                        console-login
                        dump-memory . . .
                        interface . . .
                        reboot-system . . .
```

command-completion

Utilice el mandato **enable command-completion** para habilitar la función de finalización automática de mandatos, que ayuda en la sintaxis de los mandatos. Consulte la sección “Finalización del mandato” en la página 23 para ver una explicación de la función de finalización automática de mandatos.

console-login

Habilita la solicitud de un ID de usuario y una contraseña en la consola física. Esto es útil para situaciones de seguridad. Si no configura ningún usuario administrador y habilita esta característica, aparece el mensaje siguiente:

```
Warning: Console login is disabled until an
administrative user is added.
```

Atención: Antes de habilitar el inicio de sesión de consola, guarde la configuración con el inicio de sesión de consola inhabilitado. Si la autenticación del inicio de sesión se establece en un servidor remoto que utiliza Radius o Tacacs+ y el dispositivo no puede llegar al servidor de autenticación, se deniega el acceso al dispositivo. Mediante la inhabilitación del inicio de sesión de consola, se impide una situación de bloqueo.

dump-memory

Habilita el vuelco de la memoria del sistema en el disco duro instalado si se produce un error grave. Es aconsejable para poder conservar el estado de la unidad en el momento del error para la posterior resolución del problema. La función de vuelco de memoria no puede habilitarse a menos que el re arranque del sistema esté habilitado. Si intenta habilitar la función

Mandatos CONFIG

de vuelco de memoria mientras el re arranque del sistema está inhabilitado, no se habilita la función de vuelco de memoria y se visualiza el mensaje siguiente:

```
System memory dump function not enabled: rebooting must be enabled first
```

Si ha configurado los vuelcos del sistema para guardar los 3 primeros archivos de vuelco y ya existen 3 archivos de vuelco en el disco duro, el sistema visualiza el mensaje siguiente cuando se habilita el vuelco de memoria:

```
*** System dump cannot be enabled until the      ***
*** existing dump files are deleted.            ***
```

Consulte los mandatos **set dump enable-mode** y **set dump save-mode**.

Ejemplo:

```
Config> enable dump
```

```
Current System Dump Status:
System dump is currently disabled.
Number of existing dump files: 0
```

```
Enable system memory dumping? [No]: Yes
```

```
Current System Dump Status:
System dump is currently enabled.
Number of existing dump files: 0
```

Nota: Si entra este mandato y no está disponible un disco duro, recibirá un mensaje que indica que la unidad no está disponible.

interface *númerointerfaz*

Hace que se habilite la interfaz después de emitir el mandato **reload**.

reboot-system

Habilita el re arranque del sistema cuando se produce un error grave.

Event

Utilice el mandato **event** para entrar en el entorno del Sistema de anotación cronológica de sucesos (ELS) para poder definir los mensajes que aparecerán en la consola. Consulte la sección “Capítulo 10. Utilización del Sistema de anotación cronológica de sucesos (ELS)” en la página 137 para obtener información acerca de ELS.

Sintaxis:

event

Feature

Utilice el mandato **feature** para acceder a los mandatos de configuración para características de dispositivo específicas, fuera de los procesos de configuración de interfaz de red y de protocolos.

Sintaxis:

feature *[númerocaracterística o nombre-corto-característica]*

Todas las características del 2216 tienen mandatos que se ejecutan:

- Accediendo al proceso de configuración para configurar inicialmente la característica y habilitarla, así como realizar cambios posteriores en la configuración.

Mandatos CONFIG

- Accediendo al proceso de consola para supervisar la información acerca de cada característica o realizar cambios temporales en la configuración.

El procedimiento para acceder a estos procesos es el mismo para todas las características. La información siguiente describe el procedimiento.

Entre un signo de interrogación después del mandato **feature** para obtener un listado de las características disponibles para el release de software.

Para acceder al indicador de configuración de una característica entre el mandato **feature** seguido del número de la característica o su nombre corto. La Tabla 9 lista los números y nombres de las características disponibles.

Tabla 9. Números y nombres de las características del IBM 2216

Número de característica	Nombre corto de característica	Accede al siguiente proceso de configuración de característica
0	WRS	Restauración/redireccionamiento de WAN
1	BRS	Reserva de ancho de banda
2	MCF	Filtro MAC
4	VCRM	Gestión de recursos y circuitos virtuales
7	ES	Subsistema de codificación
8	NDR	Asignador de tareas de la red
9	DIAL	Acceso de marcación de entrada a las LAN
10	AUTH	Autenticación
11	IPSec	Configuración de usuario de la característica Seguridad IP
12	LAYER	Layer 2 Tunneling Protocol, Layer 2 Filtering, Point-to-Point Tunneling Protocol
13	NAT	Configuración de usuario de Convertidor de direcciones de red
14	TSF	Función de servidor fino
15	WEBC	Antememoria de servidor web ¹
15	HOD	Antememoria de cliente Host on Demand ¹
16	DHCP	Servicios DHCP
20	POLICY	Característica de política
21	DS	Servicios diferenciados
22	RED	Detección rápida aleatoria

¹HOD y WEBC no coexisten en la misma imagen de software; por lo que tienen el mismo número de característica.

Una vez haya accedido al indicador de configuración para una característica, puede empezar a entrar los mandatos de configuración específicos para la característica. Para volver al indicador CONFIG, entre el mandato **exit** en el indicador de configuración de la característica.

List

Utilice el mandato **list** para visualizar la información de configuración para todas las interfaces de red o la información de configuración para el dispositivo.

Mandatos CONFIG

Sintaxis:

```
list
configuration
devices
named-profile
isdn-address
patches . . .
ppp_users . . .
tunnel-profile
users . . .
v25-bis-address
vpd
```

configuration

Visualiza la información de configuración del dispositivo.

Ejemplo: list configuration

```
Hostname: [none]
Maximum packet size: [autoconfigured]
Maximum number of global buffers: [autoconfigured]
Number of spare interfaces: 0
Console inactivity timer (minutes): 0
Physical console login: disabled
System rebooting on error: disabled
System memory dumping: disabled
Contact person for this node: [none]
Location of this node: [none]

Configurable Protocols:
Num Name Protocol
0 IP DOD-IP
3 ARP Address Resolution
4 DN DNA Phase IV
6 VIN Banyan Vines
7 IPX NetWare IPX
8 OSI ISO CLNP/ISIS/ISIS
9 DVM Distance Vector Multicast Routing Protocol
10 BGP Border Gateway Protocol
11 SNMP Simple Network Management Protocol
12 OSPF Open SPF-Based Routing Protocol
20 SDLC SDLC/HDLC-Relay
22 AP2 AppleTalk Phase 2
23 ASRT Adaptive Source Routing Transparent Enhanced Bridge
24 HST TCP/IP Host Services
25 LNM LAN Network Manager
26 DLS Data Link Switching
27 XTP X.25 Transport Protocol
28 APPN Advanced Peer-to-Peer Networking [HPR]
29 NHRP Next Hop Routing Protocol
30 APPN Advanced Peer-to-Peer Networking [ISR]

Configurable Features:
Num Name Feature
0 WRS WAN Restoral
1 BRS Bandwidth Reservation
2 MCF MAC Filtering
6 QOS Quality of Service
7 CMPRS Data Compression Subsystem
8 NDR Network Dispatching Router
10 AUTH Authentication
14 TSF Thin Server Function

26176 bytes of configuration memory free
```

devices [dispositivo o rangodispositivos]

Visualiza la relación entre un número de interfaz y la interfaz de hardware. También puede utilizar este mandato para comprobar que se ha añadido correctamente un dispositivo utilizando el mandato **add**.

También puede especificar un rango de dispositivos que se ha de listar, tal como muestra el ejemplo siguiente:

```
list dev 2-5
Ifc 2 Token Ring           Slot: 2 Port: 1
Ifc 3 Token Ring           Slot: 2 Port: 2
Ifc 4 Ethernet             Slot: 4 Port: 1
Ifc 5 Ethernet             Slot: 4 Port: 2
```

Nota: Si no especifica ningún número de interfaz o el rango de interfaces, se visualizan todas las interfaces.

Ejemplo: list devices

```
Ifc 0 Token Ring           Slot: 1 Port: 1
Ifc 1 Token Ring           Slot: 1 Port: 2
Ifc 2 Token Ring           Slot: 2 Port: 1
Ifc 3 Token Ring           Slot: 2 Port: 2
Ifc 4 Ethernet             Slot: 4 Port: 1
Ifc 5 Ethernet             Slot: 4 Port: 2
Ifc 6 Ethernet             Slot: 5 Port: 1
Ifc 7 Ethernet             Slot: 5 Port: 2
Ifc 8 Ethernet             Slot: 6 Port: 1
Ifc 9 Ethernet             Slot: 6 Port: 2
Ifc 10 V.35/V.36 Frame Relay Slot: 8 Port: 0
Ifc 11 V.35/V.36 X.25      Slot: 8 Port: 1
Ifc 12 V.35/V.36 PPP       Slot: 8 Port: 2
Ifc 13 V.35/V.36 PPP       Slot: 8 Port: 3
Ifc 14 V.35/V.36 PPP       Slot: 8 Port: 4
Ifc 15 V.35/V.36 PPP       Slot: 8 Port: 5
```

Nota: El número de almacenamientos intermedios de recepción indicados son excepciones de los valores por omisión de almacenamientos intermedios de recepción. El mandato **set receive buffers** se explica en la sección "Set" en la página 106.

isdn-address

Visualiza las configuraciones de direcciones RDSI actuales.

```
Ejemplo: list isdn-address
Address assigned name      Network Address      Network Subdial Address
-----
remote site XYZ           1 2345 67           98765
```

patches

Visualiza los valores de las variables de parche que se han entrado utilizando el mandato **patch**.

Ejemplo:

```
list patches
Patched variable          Value

ping-size                 60
ping-ttl                  59
ethernet-security         3
```

ppp_users

Lista parámetros de perfil de usuario PPP específicos.

Ejemplo: Lista de usuarios PPP cuando DIALs no está en la carga del software

```
Config> list ppp_users
List (Name, Verb, User, Addr, Encr):

      PPP User Name: joe
      User IP Address: Interface Default
      Encryption: Not Enabled
```

Ejemplo: Lista de usuarios PPP cuando DIALs está en la carga de software

Mandatos CONFIG

```
Config> list ppp_users
List (Name, Verb, User, Addr, Call, Time, Dial, Encr):

  PPP User Name: joe
  User IP Address: Interface Default
  Net-Route Mask: 255.255.255.255
  Hostname: <undefined>
  Time-Allotted: Box Default
  Call-Back Type: Not Enabled
  Dial-Out: Not Enabled
  Encryption: Not Enabled
```

Cuando entre **list ppp_users**, el software le solicitará que entre uno de los elementos siguientes:

Name Lista todos los nombres de la base de datos.

Verb Lista información detallada acerca de cada usuario. Lista toda la información perteneciente a cada perfil de usuario.

User Lista información detallada acerca de un solo usuario.

Addr (address)

Lista información de dirección IP para cada usuario, incluyendo la Dirección IP, la máscara de red y el nombre de sistema principal.

Call (callback)

Lista la información de llamada de retorno para cada usuario, incluyendo el tipo de llamada de retorno y el número.

Time Lista el tiempo permitido configurado para cada usuario.

Encr (encryption)

Lista si el cifrado está habilitado para cada usuario.

tunnel-profile

Visualiza los parámetros de perfil de túnel.

Ejemplo:

```
Config>list tunnel-profile

Endpoint Tunnel name Hostname
11.0.0.192 lac lns

1 TUNNEL record displayed.

Config>
```

Tunnel Name

Especifica el nombre configurado para el similar.

Server Endpoint

La dirección IP del similar.

Type Especifica el tipo de conexión similar.

Medium

Especifica el protocolo que el túnel utiliza.

Local Host Name

Especifica el nombre configurado para utilizar cuando se conecta al similar.

users Visualiza los usuarios configurados para acceder al sistema.

Ejemplo:

```
list users
USER      PERMISSION
juan      operations
maría     administrative
pedor     monitor
```

v25-bis-address

Visualiza las configuraciones actuales de direcciones V25 bis. La configuración de dirección V25 bis consta de la dirección de red y el nombre de dirección de red para un puerto local (interfaz de línea serie) o el puerto de destino. La dirección de red es el número de teléfono del puerto local o de destino. El nombre de dirección de red puede ser cualquier cosa como, por ejemplo, la descripción del puerto. Consulte la sección "Capítulo 50. Utilización de la interfaz de red V.25bis" en la página 751 para obtener más información.

```
Ejemplo:
list v25-bis-address
Address assigned name      Network Address
-----
v25-1                      8982800
v25-2                      8980001
delaware                   1-666-555-4444
```

vpd Visualiza los datos vitales del producto del hardware y del software.

Load

Utilice el mandato **load** para listar los paquetes de la carga de software que están disponibles pero no configurados o los paquetes que están configurados en la carga del software. El mandato **load** también se utiliza para añadir o suprimir un paquete de software.

Sintaxis:

```
load                add package nombrepaquete
                     delete package nombrepaquete
                     list . . .
```

El software se divide en múltiples módulos de carga. Estos módulos de carga se agrupan en paquetes de software. Algunos de estos paquetes de software son opcionales porque, aunque se suministran con el producto, no se cargan automáticamente.

Los paquetes de software que contienen cifrado están disponibles en el servidor web del 2216 que se puede acceder mediante Internet.

Para cargar y ejecutar los paquetes de software opcionales:

1. Añada el paquete utilizando el mandato **load add**.
2. Rearranque. Esta acción carga el software opcional en la memoria del dispositivo.
3. Configure el software opcional.
4. Guarde la configuración.
5. Rearranque el dispositivo. Esta acción habilita el software con la nueva configuración.

add package *nombrepaquete*

Añade un paquete de software al software. *nombrepaquete* es el nombre del paquete de los módulos de carga que desea incluir en el software.

Ejemplo: load add package appn

delete package *nombrepaquete*

Elimina un paquete de software del software. *nombrepaquete* es el nombre del paquete de módulos de carga que desea eliminar del software.

Mandatos CONFIG

Ejemplo: load delete package appn

list Lista los paquetes de la carga de software que están disponibles pero no configurados o los paquetes que están configurados en la carga de software. Puede especificar una de las opciones siguientes:

available

Lista los paquetes de software de la carga de software actual que no están configurados.

configured

Lista los paquetes de software de la carga de software actual que están configurados.

Network

Utilice el mandato **network** para entrar en el entorno de configuración de interfaces de red para las redes soportadas. Entre el número de la interfaz o de la red como parte del mandato. (Para obtener el número de la interfaz, utilice el mandato **list device** de CONFIG.) Se visualizará el indicador de configuración adecuado (por ejemplo, TKR Config>). Consulte los capítulos relativos a la configuración de interfaces de red de este manual para obtener información completa acerca de la configuración de los tipos de interfaces de red.

Sintaxis:

network *númerointerfaz*

Notas:

1. Si cambia un parámetro configurable por el usuario, puede utilizar el mandato **reset interface** de GWCON o puede volver a cargar el dispositivo para que el cambio surta efecto. Para hacerlo, entre el mandato **reload** en el indicador de OPCON (*).
2. El usuario no puede configurar todas las interfaces de red. Para las interfaces que no puede configurar, recibirá el mensaje: That network is not configurable.

Patch

Utilice el mandato **patch** para modificar la configuración global del dispositivo. Las variables de parche se registran en la memoria de configuración no volátil y surten efecto inmediatamente; no tiene que esperar al siguiente reinicio del dispositivo. Este mandato sólo debe utilizarse para manejar configuraciones que no son comunes. Lo que se configure normalmente debe seguirse manejando con los mandatos de configuración específicos. La siguiente lista contiene las variables de parche actuales documentadas y soportadas para este release.

Sintaxis:

patch *bgp-subnets*
dls-ignore-lfs
ethernet-security
filter-nr
ip-default-ttl
ip-mtu
lnm-link-via-tbport

more-lines
 mosheap-lowmark
 ospf-import-rate
 ping-size
 ping-ttl
 ppp-echo
 relax-jate
 rip-static-suppress
 tftp-max-rxto-time
 tftp-min-rexmtime

bgp-subnets *nuevo valor*

Si desea que el altavoz BGP advierta de las rutas de subred a sus direccionadores contiguos, establezca *nuevo valor* en 1. El valor por omisión es 0.

dls-ignore-lfs *nuevo valor*

Cuando se establece en 1, DLSw pasa por alto los bits del tamaño “trama mayor” de las tramas direccionadas de origen al configurar un circuito. Esto evita problemas de configuración de circuitos con algunos productos LAN antiguos que no establecen estos correctamente estos bits. El valor por omisión es 0.

ethernet-security *nuevo valor*

Cuando se establece en un valor distinto de cero, rellena con ceros los paquetes Ethernet cuya porción de datos es inferior al mínimo físico de 60 bytes. Esto puede ser necesario por razones de seguridad. Valor por omisión: 0.

filter-nr

Permite filtrar el “Nombre reconocido” de NetBIOS junto con la lista actual de tramas NetBIOS filtradas por el código puente. Los filtros de nombre NetBIOS pasarán todos los paquetes NetBIOS que no sean de uno de los tipos siguientes: ADD_GROUP_NAME_QUERY, ADD_NAME_QUERY, DATAGRAM, NAME_QUERY. Este parámetro añade NAME_RECOGNIZED a la lista de tipos.

ip-default-ttl *número_de_paquetes*

El TTL utilizado en los paquetes que el dispositivo origina. El valor por omisión es 64.

Nota: Es preferible establecer este parámetro con el mandato de configuración IP **set ttl**. (Consulte la sección “Set” del capítulo “Using and Configuring IP” de la publicación *Consulta de configuración y supervisión de protocolos Volumen 1*.) Esta variable de parche se conserva para la compatibilidad con configuraciones de releases anteriores.

ip-mtu *bytes*

Este parámetro limita el tamaño de MTU IP al valor especificado. Cuando se establece este parámetro, el tamaño de MTU IP de una interfaz de red determinada se establece en el valor menor de ip-mtu y el valor mayor que el tamaño de trama configurado de la interfaz de red puede acomodar.

Mandatos CONFIG

Inm-link-via-tbport *nuevo valor*

Permite que el LNM enlace con una red en anillo a través de un puerto de puente transparente (TB) Ethernet.

Cuando se establece en 1, el enlace LNM está permitido.

Cuando se establece en 0, el valor por omisión, no está permitido el enlace LNM.

more-lines *número_de_líneas*

El número de líneas que se ha de visualizar en la consola cuando se lista una salida larga.

mosheap-lowmark *nuevo valor*

Este parámetro especifica el porcentaje de memoria de almacenamiento dinámico MOS libre, en la que el dispositivo notifica al operador que se está quedando sin memoria. Esta notificación permite al operador liberar memoria de almacenamiento dinámico MOS antes de que el dispositivo reciba un error y se detenga.

Cuando el operador recibe la notificación, puede reconfigurar el dispositivo y, a continuación, rearrancarlo, minimizando el corte en la red. La especificación de 0 para este parámetro suprime este aviso.

Valores válidos: De 0 a 100

Valor por omisión: 10

ospf-import-rate *velocidad*

Número de rutas importadas por segundo.

ping-size *bytes*

El tamaño de la parte de datos (es decir, excluyendo las cabeceras IP e ICMP) del paquete ICMP PING que se envía mediante el mandato IP>**ping**. Valor por omisión: 56 bytes. (El tamaño de los datos PING también puede entrarse como un parámetro del mandato **ping** tal como se describe en la sección "Ping" del capítulo "Monitoring IP" de la publicación *Consulta de configuración y supervisión de protocolos Volumen 1*.)

ping-ttl *segundos*

El TTL (período de duración) enviado en los PING por el mandato IP>**ping**. Valor por omisión: 64. (El TTL también puede entrarse como un parámetro del mandato **ping**, tal como se describe en la sección "Ping" del capítulo "Monitoring IP" de la publicación *Consulta de configuración y supervisión de protocolos Volumen 1*.)

ppp-echo *nuevo valor*

Cuando se establece en 1, el dispositivo no enviará Peticiones de eco PPP en ninguna interfaz PPP. Las Peticiones de eco PPP se envían a los dispositivos remotos como parte del mantenimiento PPP para asegurarse de que el dispositivo remoto está operativo. Considere la posibilidad de habilitar esta variable cuando ejecute PPP en una línea lenta y utilizar esa línea para transmitir paquetes de datos grandes de modo que los paquetes de mantenimiento PPP no se intercambien con la suficiente frecuencia para mantener activa la interfaz PPP.

relax-jate

Libera la restricción JATE RDSI.

rip-static-suppress *nuevo valor*

Cuando se establece en un valor distinto de cero, RIP no advertirá a las rutas estáticas a través de una interfaz determinada a menos que se

proporcione el mandato `mandatoIP config> enable send static` para la interfaz. Esto cambia la semántica del mandato **enable send static**. Cuando `rip-static-suppress` es igual a 0 (el valor por omisión), la lista de las rutas anunciadas a través de RIP es la unión de las especificadas por los distintivos RIP de la interfaz.

fftp-max-rxto-time

fftp-max-rxto-time le permite especificar el tiempo máximo que se ha de esperar una respuesta del asociado antes de que la transferencia se considere anómala. **Valor por omisión:** 5 minutos

La unidad para esta variable de parche es el segundo.

fftp-min-rexmtime

fftp-min-rexmtime le permite especificar el intervalo mínimo de tiempo que se ha de esperar una respuesta del asociado antes de volver a transmitir el último paquete enviado. **Valor por omisión:** 1

La unidad para esta variable de parche es el segundo.

Nota: Debe especificar el nombre completo de la variable de parche que desea cambiar. No puede utilizar una sintaxis abreviada para el nombre de parche.

Performance

Utilice el mandato **performance** en el indicador `Config>` para entrar en el entorno de configuración para el rendimiento. Consulte la sección “Capítulo 12. Configuración y supervisión del rendimiento” en la página 213 para obtener más información.

performance

Protocol

Utilice el mandato **protocol** en el indicador `Config>` para entrar en el entorno de configuración para el software de protocolo instalado en el dispositivo.

Sintaxis:

protocol *[número_{prot} o nombre_{prot}]*

El mandato **protocol** seguido del número de protocolo deseado *o* del nombre corto le permite entrar en el entorno de mandatos de un protocolo. Después de entrar este mandato, aparece el indicador del protocolo especificado. En el indicador, puede entrar los mandatos específicos de ese protocolo. Para volver a `Config>`, entre el mandato **exit**.

Notas:

1. Para ver los nombres y los números de los protocolos que hay en la carga de software, en el indicador `Config>`, entre **list configuration**.
2. Cuando cambie un parámetro configurable por el usuario, es posible que pueda utilizar el mandato **reset** de GWCON del protocolo o puede que tenga que reiniciar el dispositivo para que el cambio surta efecto. Para hacerlo, entre el mandato **reload** en el indicador de OPCON (*).

Los cambios que realiza a través de CONFIG se guardan en la base de datos de configuración en memoria no volátil y se vuelven a llamar cuando se reinicia el dispositivo.

Mandatos CONFIG

Qconfig

Utilice el mandato **qconfig** para iniciar la Configuración rápida. La Configuración rápida le permite configurar los parámetros para el puente y el direccionamiento de protocolos sin entrar en entornos de configuración independientes.

Sintaxis:

qconfig

Nota: Para obtener una información completa sobre cómo utilizar el software de Configuración rápida proporcionado con el dispositivo, consulte el “Apéndice A. Consulta para la configuración rápida” en la página 809.

Set

Utilice el mandato **set** para configurar diversos parámetros de todo el sistema.

Sintaxis:

set contact-person . . .
data-link . . .
down-notify . . .
dump enable-mode
dump save-mode
global-buffers
hostname
inactivity-timer
input-low-water
location . . .
logging level
packet-size
prompt
receive-buffers
spare-interfaces

contact-person *contactoSis*

Establece el nombre o identificación de la persona de contacto para este nodo SNMP gestionado. Existe un límite de 80 caracteres para la longitud del nombre de *contactoSis*.

Esta variable sólo sirve para propósitos informativos y no tiene ningún efecto en el funcionamiento del dispositivo. Es útil para la identificación de la gestión SNMP del sistema.

data-link *tipo númerointerfaz*

Seleccione el tipo de enlace de datos para una interfaz serie o una interfaz de circuito de marcación. El *tipo* puede ser:

- FRAME-RELAY
- PPP
- SDLC
- SRLY

- V25BIS
- X25

Notas:

1. PPP, SDLC y Frame Relay son los únicos enlaces de datos soportados en interfaces de circuito de marcación. X.25 sólo está soportado en el canal D RDSI BRI.
2. Pueden utilizarse todos los tipos de enlaces de datos en el adaptador EIA 232E de 8 puertos, en el adaptador V.35/V.36 de 6 puertos y en el adaptador X.21 de 8 puertos excepto V.25bis que sólo puede utilizarse con el adaptador EIA 232E.

númeroInterfaz es el número de la interfaz que está configurando.

down-notify *númerointerfaz* *número de segundos*

Permite al usuario especificar el número de segundos antes de declarar que una interfaz está desactivada. El intervalo normal del paquete de mantenimiento es de 3 segundos y son necesarias cuatro anomalías de mantenimiento para declarar que la interfaz está desactivada.

El mandato **set down-notify** se utiliza principalmente cuando el tráfico LLC pasa por túnel a través de una red IP utilizando OSPF. Si se desactiva una interfaz, OSPF no puede detectarlo con la suficiente rapidez debido al período de tiempo que tarda en declarar desactivada una interfaz. Por lo tanto, las sesiones LLC empezarían a exceder tiempos de espera. Puede establecer el temporizador de notificación de desactivación en un valor inferior, permitiendo que OSPF detecte que una interfaz está desactivada más rápidamente. Esto permite elegir una ruta alternativa más rápidamente, lo que impide que las sesiones LLC excedan el tiempo de espera.

Nota: Si se ejecuta el mandato **set down-notify** en un extremo de un enlace serie, debe ejecutarse el mismo mandato en el otro extremo del enlace o puede que el enlace no se active y permanezca activado.

númeroInterfaz

El número de la interfaz que está configurando.

número de segundos

El valor de tiempo de notificación de desactivación que especifica el tiempo máximo que transcurrirá antes de que una interfaz desactivada se marque como tal. Los valores grandes provocarán que el dispositivo pase por alto problemas de conexión transitorios y los valores inferiores provocarán que el dispositivo reaccione más rápidamente. El rango de valores es de 1 a 300 segundos y el valor por omisión es 0, lo que establece el período de 3 segundos. El establecimiento del tiempo de notificación de desactivación en 0 restaurará el tiempo por omisión para esta interfaz.

El mandato **list devices** mostrará el valor del tiempo de notificación de desactivación para cualquier interfaz cuyo valor por omisión se haya alterado temporalmente.

dump enable-mode

Especifica si se habilita el vuelco después del siguiente vuelco del sistema. Si configura la modalidad de guardar (consulte el mandato **set dump save-mode**) para guardar los tres primeros vuelcos y el sistema ya ha

Mandatos CONFIG

creado el tercer archivo de vuelco, se inhabilitan los vuelcos sin tener en cuenta la especificación. En el momento en que el sistema crea el tercer archivo de vuelco, recibirá el mensaje siguiente:

```
Active Dump Detected.  
Dump Compression in Progress, please be patient ...  
  
*** System dumping is being DISABLED because dumping is ***  
*** configured to save the 3 initial dumps, but 3 ***  
*** dump files already exist. ***
```

Ejemplo:

```
Config> set dump enable-mode  
  
Current System Dump Settings:  
  Disable System Dump following the next system dump.  
  Save the last 3 (most recent) dump files.  
  
Do you want to change system dump enable-mode to  
re-enable System Dump following the next system dump ? (Yes, No): [No] Yes  
  
Current System Dump Settings:  
  Re-enable System Dump following the next system dump.  
  Save the last 3 (most recent) dump files.  
  
Current System Dump Status:  
  System dump is currently enabled.  
  Number of existing dump files: 2
```

Valor por omisión: inhabilitado

Nota: Los vuelcos se habilitan con el mandato **enable dump-memory**.

dump save-mode

Especifica si se han de guardar los tres primeros (iniciales) archivos de vuelco del sistema o los tres últimos (más recientes). Consulte **dump enable-mode** para ver la consideración de utilizar la modalidad más reciente en lugar de la modalidad inicial.

Ejemplo:

```
Config> set dump save-mode  
  
Current System Dump Settings:  
  Re-enable System Dump following the next system dump.  
  Save the last 3 (most recent) dump files.  
  
Do you want to change system dump save-mode to  
save the first (initial) dump files ? (Yes, No): [No] Yes  
  
Current System Dump Settings:  
  Re-enable System Dump following the next system dump.  
  
  Save the first 3 (initial) dump files, then disable system dump.  
  
Current System Dump Status:  
  System dump is currently enabled.  
  Number of existing dump files: 2
```

Valor por omisión: reciente

global-buffers *númeromáx*

Establece el número máximo de almacenamientos intermedios de paquetes globales, que son los almacenamientos intermedios de paquetes utilizados para los paquetes originados localmente. El valor por omisión es configurar automáticamente el número máximo de almacenamientos intermedios (10000 como máximo). Para restaurar el valor por omisión, establezca el valor en 0. Para visualizar el valor para los almacenamientos intermedios globales, utilice el mandato **list configuration**.

hostname *nombre*

Añade o cambia el nombre de dispositivo. El nombre de dispositivo sirve sólo como identificación; no afecta a ninguna dirección de dispositivo. El *nombre* debe tener menos de 78 caracteres y es sensible a las mayúsculas y minúsculas.

inactivity-timer *número_de_min*

Cambia el valor del Temporizador de inactividad. El Temporizador de inactividad finaliza la sesión de un usuario si la consola física o remota está inactiva durante el período de tiempo especificado en este mandato. Este mandato sólo afecta a las consolas que necesitan inicio de sesión. El valor por omisión de 0 desactiva el temporizador de inactividad, indicando que no se realiza ningún fin de sesión, no importa el tiempo que la consola permanezca inactiva.

input-low-water *númerointerfaz**número_mínimo_de_almacenamientos_intermedios_de_recepción*

Le permite configurar un umbral mínimo de interfaz para los almacenamientos intermedios de recepción. Cuando el número actual de almacenamientos intermedios de recepción para una interfaz es menor que el umbral mínimo de la interfaz, se puede elegir el paquete para el control de flujo (eliminación) si el paquete está en cola una cola de salida que ha alcanzado el valor máximo de umbral (equidad). Consulte la descripción del mandato **queue** de GWCON para obtener más detalles sobre el control del flujo.

Si se reduce el valor de umbral mínimo será menos probable que se eliminen los paquetes de esta interfaz cuando se envíen en redes congestionadas. Sin embargo, si se reduce el valor puede afectar negativamente al rendimiento si se producen pérdidas de datos por defecto debido a que la cola del almacenamiento intermedio de recepción está vacía. La elevación del valor tiene el efecto opuesto. Para determinar si se producen pérdidas de datos por defecto, utilice el mandato **interface** de GWCON y especifique el número de interfaz. Para determinar si se están desactivando paquetes de esta interfaz debido a que se ha alcanzado el umbral mínimo, utilice el mandato **error** de GWCON (Talk 5) y consulte el valor del contador de Eliminar flujo para la interfaz.

El rango de valores va de 1 a 255. El valor por omisión es específico del producto y específico del dispositivo. El umbral mínimo debe ser menor que el número pedido de almacenamientos intermedios de recepción. La especificación del valor 0 restaura el valor por omisión de configurado automáticamente.

Utilice los mandatos **buffer** y **queue** de GWCON (Talk 5) para mostrar el valor de umbral mínimo.

númeroInterfaz es el número de la interfaz que está configurando.

número_mínimo_de_almacenamientos_intermedios_de_recepción es el valor del umbral mínimo.

location *ubicaciónSist*

Establece la ubicación física de un nodo SNMP. Existe el límite de 80 caracteres para la longitud del nombre de *ubicaciónSist*. Esta variable sólo sirve para propósitos informativos y no tiene ningún efecto en el funcionamiento del dispositivo. Es útil para la identificación de la gestión SNMP del sistema.

logging level *número*

Controla la salida de los mensajes que todavía no se han convertido a

Mandatos CONFIG

ELS. (Consulte para obtener más información acerca de ELS.) El nivel de anotación cronológica se registra en la configuración. Cuando se enciende el dispositivo o se reinicia, el nivel de anotación cronológica surte efecto y determina la salida de mensajes. El nivel de anotaciones cronológicas por omisión es 76. El nivel de anotaciones cronológicas 0 es igual a ningún nivel de anotación cronológica.

Ejemplo: `set logging level 76`

packet-size *tamaño_máx_paquete_en_bytes*

Establece o cambia el tamaño máximo para los almacenamientos intermedios globales y los almacenamientos intermedios de recepción. Si especifica el valor 0 como el tamaño máximo de paquete, el tamaño de los almacenamientos intermedios de recepción para una interfaz se basa en el tamaño de paquete configurado en esa interfaz y el tamaño de paquete de los almacenamientos intermedios globales se configuran automáticamente. Si especifica un valor que no es cero, se utiliza el valor configurado como el tamaño de paquete de almacenamiento intermedio global y cualquier interfaz que tenga un tamaño de paquete configurado que sea mayor que el tamaño máximo de paquete utilizará el tamaño máximo de paquete para sus almacenamientos intermedios de recepción. El valor 0 (para configurar automáticamente) es el valor por omisión.

Atención: Utilice este mandato únicamente bajo instrucciones directas del servicio técnico. No lo utilice *nunca* para reducir el tamaño de paquete – *sólo* para aumentarlo.

prompt *nombre-definido-usuario*

Añade un nombre definido por el usuario como prefijo a todos los indicadores del operador, sustituyendo el nombre de sistema principal.

El nombre-definido-usuario puede ser cualquier combinación de caracteres, números y espacios hasta un máximo de 80 caracteres. Pueden utilizarse caracteres especiales para pedir funciones adicionales, tal como se describe en la Tabla 10.

Ejemplo:

```
set prompt
What is the new MOS prompt [y]? AnyHost 99
AnyHost 99 Config>
```

Tabla 10. Funciones adicionales proporcionadas por el mandato de establecer nivel de indicador

Caracteres especiales	Función proporcionada por el mandato de establecer nivel de indicador
\$n	Visualiza el nombre de sistema principal. Es útil cuando se desea que el nombre del sistema principal se incluya en el indicador. Por ejemplo: Config> set prompt What is the new MOS prompt [y]? \$n nombresistemaprincipal:: Config>
\$t	Visualiza la hora. Por ejemplo: Config> set prompt . What is the new MOS prompt [y]? \$t 02:51:08[GMT-300] Config>
\$d	Visualiza fecha-mes-año actuales. Por ejemplo: Config> set prompt . What is the new MOS prompt [y]? \$d 26-Feb-1997 Config>

Tabla 10. Funciones adicionales proporcionadas por el mandato de establecer nivel de indicador (continuación)

Caracteres especiales	Función proporcionada por el mandato de establecer nivel de indicador
\$v	Visualiza la información de los VPD del software en el formato siguiente: programa-producto-nombre Característica xxxx Vx Rx.x PTFx RPQx
\$e	Borra un carácter <i>después</i> de esta combinación en el indicador definido por el usuario.
\$h	Borra un carácter <i>antes</i> de esta combinación en el indicador definido por el usuario.
\$_	Añade un retorno de carro al indicador definido por el usuario.
\$\$	Visualiza \$.
<p>Nota: Puede combinar estos mandatos. Por ejemplo:</p> <pre>Config> set prompt What is the new MOS prompt [y]? \$n::\$d nombresistemaprincipal::26-Feb-1997 Config></pre>	

receive-buffers númerointerfaz número máx

Ajusta el número de almacenamientos intermedios de recepción privados para la mayoría de interfaces para aumentar el rendimiento de recepción de una interfaz y para reducir las eliminaciones del control de flujo cuando el direccionador reenvía muchos paquetes desde una interfaz rápida a una interfaz lenta. El rango de valores va de 5 a 4096. Para restaurar el valor por omisión, especifique un valor 0. No todos los tipos de dispositivo permiten configurar el número máximo de almacenamientos intermedios de recepción ni soportan 4096 almacenamientos intermedios de recepción. Utilice la Tabla 11 para determinar el valor por omisión y el máximo para cada tipo de dispositivo. Este mandato no impone los valores máximos mostrados en la Tabla 11. Le permite configurar un valor máximo que no esté soportado por un dispositivo.

El efecto de este mandato lo muestra el mandato **buffer** de GWCON. Si configura un valor máximo válido, este valor aparece en la columna Input Req de la salida del mandato **buffer** de GWCON. Si configura un valor máximo que el dispositivo no soporta, el mandato **buffer** de GWCON muestra el número por omisión de almacenamientos intermedios de recepción en la columna Input Req y se anota cronológicamente un mensaje ELS de subsistema GW.

Nota: Este mandato no se aplica a las Interfaces de velocidad primaria RDSI. Para RDSI PRI, el número de almacenamientos intermedios de recepción se fija en 5 por canal B, 115 para T1 y 150 para E1. Cuando se está en modalidad canalizada, la PRI tiene 5 almacenamientos intermedios de recepción por período de tiempo configurado.

Tabla 11. Valores por omisión y máximos para interfaces

Interfaz	Valor por omisión	Máximo
ATM	80 *	4096 **
Ethernet de 10 Mbps	40*	1000
Ethernet de 10/100 Mbps	64*	1000
Serie	24	250
TKR	40*	1000

Mandatos CONFIG

Tabla 11. Valores por omisión y máximos para interfaces (continuación)

Interfaz	Valor por omisión	Máximo
FDDI	80	80
HSSI	60*	1000
ESCON	1000	1000
PCA	1000	1000

* Este es el valor por omisión para 2216-400. Para Network Utility, el valor por omisión es 1000

****Importante:** Aumente este valor con cuidado. Un rango de 80 a 120 almacenamientos intermedios de recepción da como resultado un rendimiento mejor de un número limitado de conexiones ATM medido en paquetes por segundo de productividad. Si se establece un valor demasiado grande para los direccionadores con memoria del sistema limitada puede impedir que el direccionador se arranque y funcione correctamente. Por ejemplo, un direccionador con 64 MB de memoria no se ejecutará con 4 KB de almacenamientos intermedios configurados.

spare-interfaces *n*

Define *n*, el número de interfaces de repuesto, para este dispositivo. Consulte la sección "Configuración de interfaces de repuesto" en la página 71 para obtener información adicional.

Recuperación del sistema

Utilice el mandato **system retrieve** para recuperar uno o varios archivos de imagen de la memoria desde la unidad de disco duro instalada después de que se haya producido un error grave.

Sintaxis:

system *_*retrieve

Utilice TFTP para enviar archivos de imágenes de memoria seleccionados a un sistema principal remoto. El sistema le solicitará la dirección IP y los nombres de archivo del sistema principal remoto.

Si no hay archivos de vuelco, recibirá el mensaje siguiente:

```
No dump files exist to retrieve
```

Ejemplo:

```
Config> system retrieve
```

```
Current System Dump Settings:
```

```
Re-enable System Dump following the next system dump.
```

```
Save the first 3 (initial) dump files, then disable system dump.
```

```
3 dump files currently exist.
```

```
Do you want to see a summary of the dump files ? (Yes, No): [No] No
```

```
Destination IP address [0.0.0.0]? 9.9.9.1
```

```
Filename: core0.cmp
```

```
Dump Date: Tue May 05 14:38:59 1998
```

```
Do you want to retrieve this file ? (Yes, No): [No] Yes
```

Fully qualified destination path/file name [/tmp/dump0.cmp]?
The memory image file is 19.3 Mb long.

Proceed? [No]: **Yes**
Sending memory image file by tftp
TFTP transfer of /hd0/core0.cmp complete, size=20331888 status: OK
tftp transfer completed successfully.

Filename: core1.cmp
Dump Date: Wed May 06 07:53:51 1998

Do you want to retrieve this file ? (Yes, No): [No]

Filename: core2.cmp
Dump Date: Wed May 06 09:14:55 1998

Do you want to retrieve this file ? (Yes, No): [No]

System View

Utilice el mandato **system view** para visualizar los valores actuales del vuelco del sistema y el estado de los vuelcos del sistema, incluyendo cuántos archivos de vuelco existen. También puede visualizar un resumen de los archivos de vuelco.

Sintaxis:

system view

Ejemplo:

Config> **system view**

Current System Dump Settings:
Re-enable System Dump following the next system dump.
Save the first 3 (initial) dump files, then disable system dump.

Current System Dump Status:
System dump is currently enabled.
Number of existing dump files: 2

Do you want to see a summary of the dump files ? (Yes, No): [No] **Yes**

Filename: core0.cmp

Dump Date: Tue May 05 14:38:59 1998

Fatal messages:
Data St. Excp Reading 0x6c6966b1 at 0x3090fca4 in thread MOSDBG (0x304d54)

CMVC Build: cc_144b
Builder: build
Build Name: LML.1d
Retain Name: MAS.DF1
Product Number: 2216-MAS
Build Date: Wed May 6 11:47:03 1998

Filename: core1.cmp

Dump Date: Wed May 06 07:53:51 1998

Fatal messages:
Data St. Excp Reading 0x6c6966b1 at 0x3090fca4 in thread MOSDBG (0x304d54)

CMVC Build: cc_144b
Builder: build

Mandatos CONFIG

Build Name: LML.1d
Retain Name: MAS.DF1
Product Number: 2216-MAS
Build Date: Wed May 6 11:47:03 1998

Time

Utilice el mandato **time** para establecer la fecha y el reloj del sistema del 2216 y para visualizar los valores en la consola del usuario. Estos valores se pueden utilizar para indicar la hora en los mensajes ELS.

Nota: El 2216 tiene un reloj en el hardware que conserva la fecha y la hora después de la reinicialización.

Sintaxis:

```
time                host . . .  
                    list  
                    offset  
                    set . . .  
                    source-address . . .  
                    sync . . .
```

host *dirección_IP*

Establece la dirección IP del sistema principal que cumple con RFC 868 que se utilizará como fuente horaria. Se trata de la dirección de un sistema principal que responderá a un datagrama vacío en el puerto 37 de UDP con un datagrama que contiene la hora actual.

list Visualiza los parámetros configurados relacionados con la hora. Incluyen la hora actual (si está establecida) y la fuente horaria (operador o dirección IP del que se ha recibido la hora la última vez).

```
Ejemplo: time list  
05:20:27 Wednesday December 7, 1994  
Set by: operator  
Time Host: 131.210.4.1  
Sync Interval: 10 seconds GMT  
Offset: -300 minutes
```

offset *minutos*

Define la zona horaria, en minutos, desplazamiento de GMT (Hora Media de Greenwich). Observe que los valores del oeste de GMT son negativos. Por ejemplo, EST es 5 horas antes que GMT, por lo que el mandato sería **time offset -300**.

Valores válidos: De -720 a 720

Valor por omisión: 0

set *<año mes fecha hora minuto segundo>*

Le solicita que establezca la hora actual. Si no especifica la hora completa en el mandato, se solicitan los valores restantes. Puede cambiar la fecha, tal como se muestra en el ejemplo siguiente.

```
Ejemplo: time set  
year [1996] 1997  
month [12]?  
date [6]? 7  
hour [11]? 12  
minute [3]?  
second [2]?
```

source-address *dirección_IP*

Establece la dirección IP de la fuente UDP de los paquetes de datos del servidor de la hora.

sync *segundos*

Establece el período, en segundos, en que el dispositivo sondeará la hora actual en el sistema principal de la hora.

Unpatch

Utilice el mandato **unpatch** para restaurar los valores de las variables de parche entradas con el mandato **patch** a sus valores por omisión. Consulte el mandato **patch** en la sección “Patch” en la página 102 para ver los detalles.

Sintaxis:

unpatch *nombre_variable*

Nota: *Debe* especificar el nombre completo de la variable de parche que se ha de restaurar.

Update

Utilice el mandato **update** para actualizar la memoria de configuración cuando reciba una nueva carga de software.

Sintaxis:

update *_version-of-SRAM*

Siga las instrucciones de la nota del release proporcionada con el software. El mandato **update** es el último mandato que se entra cuando se carga un nuevo software. Después de entrar este mandato, la consola visualiza un mensaje indicando la memoria de configuración que se está actualizando.

Write

Utilice el mandato **write** para guardar la configuración en el dispositivo antes de volverlo a cargar.

Sintaxis:

write

Si no puede emitir el mandato **write** e intenta volver a cargar el dispositivo, se le solicitará si desea guardar la configuración. La configuración se guarda en el siguiente CONFIG del disco duro en el banco que está utilizando actualmente.

Mandatos CONFIG

Capítulo 8. El proceso de operación/supervisión (GWCON - Talk 5) y sus mandatos

Este capítulo describe el proceso GWCON e incluye las secciones siguientes:

- “¿Qué es GWCON?”
- “Entrada y salida de GWCON”
- “Mandatos GWCON” en la página 118

¿Qué es GWCON?

El proceso de Consola de pasarela (supervisión), GWCON (al que también se hace referencia como CGWCON), es un proceso de segundo nivel de la interfaz de usuario de dispositivo.

Mediante los mandatos GWCON, puede:

- Listar los protocolos y las interfaces configurados actualmente en el dispositivo.
- Visualizar las estadísticas de la memoria y de la red.
- Establecer los parámetros actuales del Sistema de anotación cronológica de sucesos (ELS).
- Probar una interfaz de red especificada.
- Comunicarse con procesos de tercer nivel, incluyendo los entornos de protocolo.
- Habilitar e inhabilitar interfaces.

La interfaz de mandatos GWCON se compone de niveles llamados modalidades. Cada modalidad tiene su propio indicador. Por ejemplo, el indicador para el protocolo SNMP es `SNMP>`.

Si desea saber el proceso y la modalidad con los que se está comunicando, pulse **Intro** para visualizar el indicador. Algunos mandatos de este capítulo como, por ejemplo, **network** y **protocol**, le permiten acceder a las diversas modalidades de GWCON.

Entrada y salida de GWCON

Para entrar en GWCON desde OPCON (*), elija uno de los métodos siguientes:

1. Entre el mandato **console** de OPCON:
* `console`
2. En el indicador OPCON, entre el mandato **status** para buscar el PID de GWCON. (Consulte la página 9 para ver una salida de ejemplo del mandato **status**.)
* `status`

Después, entre el mandato **talk** seguido del número PID para GWCON:

* `talk 5`

La consola visualiza el indicador GWCON (+). Si no aparece el indicador, pulse **Intro**. Ahora puede entrar mandatos GWCON.

Para volver a OPCON, entre el carácter de interceptación OPCON. (El valor por omisión es **Control-P**.)

Mandatos GWCON

Esta sección contiene los mandatos GWCON. Cada mandato incluye una descripción, los requisitos de su sintaxis y un ejemplo. Los mandatos GWCON se resumen en la Tabla 12.

Para utilizar los mandatos GWCON, acceda al proceso GWCON entrando **talk 5** y entre los mandatos GWCON en el indicador (+).

Tabla 12. Resumen de los mandatos GWCON

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado "Cómo obtener ayuda" en la página 10.
Activate	Habilita una interfaz de repuesto que se acaba de configurar.
Buffer	Visualiza información acerca de los almacenamientos intermedios de paquetes asignados a cada interfaz.
Clear	Borra las estadísticas de red.
Configuration	Lista el estado de los protocolos e interfaces actuales.
Disable	Pone fuera de línea la interfaz o ranura especificada.
Disk	Lista, recupera y suprime archivos relacionados con el servicio.
Enable	Habilita todas las interfaces.
Error	Visualiza cuentas de errores.
Event	Entra en el entorno del Sistema de anotación cronológica de sucesos.
Feature	Proporciona acceso a los mandatos de consola para características de dispositivo independientes, fuera de los procesos de consola de interfaz de red y protocolo actuales.
Interface	Visualiza las estadísticas de hardware de red o las estadísticas para la interfaz especificada.
Memory	Visualiza los datos de memoria, almacenamiento intermedio y paquete.
Network	Entra en el entorno de consola de la red especificada.
Performance	Proporciona una instantánea de las estadísticas de utilización del procesador principal.
Protocol	Entra en el entorno de mandatos del protocolo especificado.
Queue	Visualiza las estadísticas de almacenamiento intermedio para una interfaz especificada.
Reset	Inhabilita la interfaz especificada y, después, vuelve a habilitarla utilizando nuevos parámetros de configuración de interfaz, protocolo y características.
Statistics	Visualiza las estadísticas para una interfaz especificada.
Test	Habilita una interfaz inhabilitada o prueba la interfaz especificada.
Uptime	Visualiza las estadísticas de tiempo para el dispositivo.

Activate

Utilice el mandato **activate** para habilitar una interfaz de repuesto en este dispositivo. Consulte la sección "Configuración de interfaces de repuesto" en la página 71 para obtener más información.

Sintaxis:

activate *númerointerfaz*

Buffer

Utilice el mandato **buffer** para visualizar información acerca de los almacenamientos intermedios de paquetes para cada interfaz o rango de interfaces.

Nota: Cada almacenamiento intermedio de un dispositivo tiene el mismo tamaño y se crea dinámicamente. El tamaño de los almacenamientos intermedios varía de un dispositivo a otro.

Para visualizar información acerca de una sola interfaz, entre el número de interfaz o de red como parte del mandato. Para obtener el número de interfaz, utilice el mandato **configuration** de GWCON.

Sintaxis:

buffer [*númerored* o *rango_de_númerored*]

Para visualizar información acerca de múltiples interfaces, especifique el *rango_de_númerored* (o una combinación de *númerored* y *rango_de_númerored*). Por ejemplo, si especifica **buffer 0 3 25-50** se visualiza la información para las redes 0, 3 y 25 a 50.

Ejemplo:

```
buffer
      Input  Buffers:      Buffer sizes:
Nt Interface Req Alloc Low Curr Hdr Wrap Data Trail Total Bytes Alloc
0  TKR/0    20   20   7   0  109  92  2052  7  2260  45200
1  PPP/0    20   20   7   20 109  92  2052  7  2260  45200
2  PPP/1    10   10   4   0  108  92  2048  0  2248  22480
```

Nt Número de interfaz de red asociada con el software.

Interface

Tipo de interfaz.

Input Buffers:

Req Número de almacenamientos intermedios de recepción pedidos. Es el número por omisión de almacenamientos intermedios de recepción del dispositivo o un valor válido establecido con el mandato **set receive-buffers** de CONFIG (Talk 6).

Notas:

1. Si esta columna es 0 para una interfaz, se trata de una interfaz virtual para la cual no se asignan almacenamientos intermedios. En este caso, la interfaz virtual utiliza los almacenamientos intermedios de recepción del dispositivo con el que correlaciona. Por ejemplo, una interfaz de circuito de marcación utiliza los almacenamientos intermedios de recepción de su red base o interfaz.
2. Si especifica un valor en el mandato **set receive-buffers** de CONFIG que el dispositivo no soporta, el número de almacenamientos intermedios pedidos es igual al número por omisión de almacenamientos intermedios de recepción del dispositivo.

Alloc Número de almacenamientos intermedios de recepción asignados.

Nota: El número de almacenamientos intermedios de recepción asignados es menor que el número de almacenamientos intermedios de

Mandatos GWCON

recepción pedidos si no hay suficiente memoria disponible para asignar el número pedido de almacenamientos intermedios.

- Low** El umbral mínimo del dispositivo para almacenamientos intermedios de recepción. Cuando el número actual de almacenamientos intermedios de recepción (entrada) para una interfaz es menor que el umbral mínimo de la interfaz, se puede elegir el paquete para control de flujo (eliminación). Consulte la descripción del mandato **queue** de GWCON (Talk 5) para obtener más detalles sobre el control de flujo. El umbral mínimo se puede configurar utilizando el mandato **set input-low-water** de CONFIG (Talk 6).
- Curr** El número actual de almacenamientos intermedios de este dispositivo. El valor será 0 si el dispositivo está inhabilitado. Cuando se recibe un paquete, si el valor de *Curr* está por debajo de *Low*, se puede elegir el paquete para el control de flujo. (Consulte el mandato **queue** para ver las condiciones.)

Buffer Sizes:

- Hdr** Suma del número máximo de cabeceras de hardware, MAC y de enlace de datos.
- Wrap** Permiso otorgado para las cabeceras de capa MAC, LLC o red debido al reinicio del protocolo.
- Data** Tamaño máximo del paquete de capa de enlace de datos.
- Trail** Suma de las colas más grandes MAC y de hardware.
- Total** Tamaño global de cada almacenamiento intermedio de paquetes.

Bytes Alloc

Cantidad de memoria de almacenamiento intermedio para este dispositivo. Este valor se determina multiplicando los valores *Alloc* x *Total*.

Clear

Utilice el mandato **clear** para suprimir la información de estadísticas acerca de una o todas las interfaces de red del dispositivo. Este mandato es útil cuando se hace un seguimiento de los cambios en contadores grandes. La utilización de este mandato no ahorra espacio ni acelera el dispositivo.

Entre el número de interfaz (o red) como parte del mandato. Para obtener el número de interfaz, utilice el mandato **configuration**.

Sintaxis:

clear *númerointerfaz* o *rango_de_númerointerfaz*

Para borrar la información acerca de múltiples interfaces, especifique el *rango_de_númerored* (o una combinación de *númerointerfaz* y *rango_de_númerointerfaz*). Por ejemplo, si especifica **clear 0 3 25-50**, se borra la información para las redes 0, 3 y 25 a 50.

Configuration

Utilice el mandato **configuration** para visualizar la información acerca de los protocolos e interfaces de red. La salida se visualiza en tres secciones, la primera sección lista la identificación del dispositivo, la versión del software, la versión ROM de arranque y el estado del conmutador de arranque automático. La segunda y tercera sección listan la información de protocolo e interfaz.

Sintaxis:**configuration**

Para visualizar información acerca de múltiples interfaces, especifique el `rango_de_númerored` (o una combinación de `númerored` y `rango_de_númerored`). Por ejemplo, la especificación de **configuration 0 3 25-50** visualiza la información para las redes 0, 3 y 25 a 50.

Ejemplo:**configuration**

```
Multiprotocol Access Services
```

```
2216-MAS Feature 2822 V3.2 Mod 0 PTF 0 RPQ 0 MAS.EF9 cc4_2a
```

```
Num Name Protocol
0 IP DOD-IP
3 ARP Address Resolution
4 DN DNA Phase IV
6 VIN Banyan Vines
7 IPX NetWare IPX
10 BGP Border Gateway Protocol
11 SNMP Simple Network Management Protocol
12 OSPF Open SPF-Based Routing Protocol
22 AP2 AppleTalk Phase 2
23 ASRT Adaptive Source Routing Transparent Enhanced Bridge
26 DLS Data Link Switching
27 XTP X.25 Transport Protocol
28 APPN Advanced Peer-to-Peer Networking [HPR]
30 APPN Advanced Peer-to-Peer Networking [ISR]
```

```
Num Name Feature
2 MCF MAC Filtering
```

```
16 Networks:
Net Interface MAC/Data-Link Hardware State
0 TKR/0 Token-Ring/802.5 Token-Ring Up
1 TKR/1 Token-Ring/802.5 Token-Ring Up
2 TKR/2 Token-Ring/802.5 Token-Ring Up
3 TKR/3 Token-Ring/802.5 Token-Ring Up
4 Eth/0 Ethernet/IEEE 802.3 Ethernet Up
5 Eth/1 Ethernet/IEEE 802.3 Ethernet Up
6 Eth/2 Ethernet/IEEE 802.3 Ethernet Up
7 Eth/3 Ethernet/IEEE 802.3 Ethernet Up
8 Eth/4 Ethernet/IEEE 802.3 Ethernet Up
9 Eth/5 Ethernet/IEEE 802.3 Ethernet Up
10 FR/0 Frame Relay V.35/V.36 Up
11 X25/0 X.25 V.35/V.36 Up
12 PPP/0 Point to Point V.35/V.36 Up
13 PPP/1 Point to Point V.35/V.36 Up
14 PPP/2 Point to Point V.35/V.36 Up
15 PPP/3 Point to Point V.35/V.36 Up
```

- La primera línea proporciona el nombre del producto.
- La segunda línea lista el número de programa/producto, el número de característica, la versión, el release y la información de PTF y RPQ.
- Las líneas restantes listan los protocolos configurados, seguidos por las características configuradas.

Se visualiza la siguiente información para los protocolos:

Num Número que se asocia con el protocolo.

Name Nombre abreviado del protocolo.

Protocol

Nombre completo del protocolo.

Se visualiza la siguiente información para las características:

Mandatos GWCON

Num Número asociado con la característica.

Name Nombre abreviado de la característica.

Feature

Nombre completo de la característica.

Se visualiza la siguiente información para las redes:

Net Número de red que el software asigna a la interfaz. Las redes se numeran empezando por 0. Estos números corresponden a los números de interfaz explicados bajo el proceso CONFIG.

Interface

Nombre de la interfaz y la instancia de este tipo de interfaz.

MAC/Data Link

Tipo de enlace de MAC/Datos configurado para la interfaz.

Hardware

Clase específica de interfaz por tipo de hardware.

State Estado actual de la interfaz de red.

Testing

Indica que la interfaz se está sometiendo a una autoprueba. Se produce cuando se inicia el dispositivo por primera vez, cuando se detecta un problema en la interfaz o cuando se utiliza el mandato **test**. (El mandato **enable slot** también puede utilizarse para iniciar una autoprueba de todas las interfaces de un adaptador.)

Cuando una interfaz está operativa, envía periódicamente paquetes de mantenimiento y/o comprueba el estado físico del puerto o línea para asegurarse de que la interfaz sigue funcionando correctamente. Si el mantenimiento falla, la interfaz se declara desactivada y se planifica la ejecución de una autoprueba para dentro de 5 segundos. Si falla una autoprueba, las transiciones de la interfaz al estado desactivado y el intervalo hasta la siguiente autoprueba se aumenta hasta un máximo de 2 minutos. Si la autoprueba es satisfactoria, la red se declara activa.

Up Indica que la interfaz está operativa.

Down Indica que la interfaz no está operativa y que ha fallado una autoprueba. La red pasará periódicamente al estado de prueba para determinar si la interfaz puede volver a estar operativa.

Disabled

Indica que la interfaz está inhabilitada. Se puede inhabilitar una interfaz mediante los métodos siguientes:

- Se puede configurar una interfaz como inhabilitada utilizando el mandato **disable** de CONFIG. Cada vez que se reinicializa el dispositivo, se inhabilitará el estado inicial de la interfaz. Permanecerá en estado inhabilitado hasta que se efectúe una acción para habilitarla.
- Se puede inhabilitar una interfaz utilizando el mandato **disable** de GWCON. Este método es temporal porque la interfaz revertirá a su estado configurado (habilitado o inhabilitado) cuando se reinicialice el dispositivo.

Mandatos GWCON

- El gestor de la red puede inhabilitar la interfaz mediante SNMP. Este método es temporal porque la interfaz revertirá a su estado configurado (habilitado o inhabilitado) cuando se reinicialice el dispositivo.

Cuando se inhabilita una interfaz, permanece inhabilitada hasta que se utiliza uno de los métodos siguientes para habilitarla:

- Se utiliza el mandato **test** de GWCON para iniciar una autoprueba de la interfaz.
- Se utiliza el mandato **enable slot** de GWCON para iniciar una autoprueba de todas las interfaces de un adaptador.
- El gestor de la red inicia una autoprueba de la interfaz mediante SNMP.

El Redireccionamiento de WAN también puede cambiar el estado de una interfaz inhabilitada. Si se configura una interfaz como alternativa para el Redireccionamiento de WAN y el estado configurado es inhabilitado, el Redireccionamiento de WAN iniciará una autoprueba de la interfaz cuando se desactive la interfaz. Cuando la interfaz primaria vuelve a estar operativa y estable, el Redireccionamiento de WAN vuelve a poner la interfaz alternativa en su estado configurado. Consulte la sección La característica redireccionamiento de WAN de la publicación *Utilización y configuración de las características* para obtener más información.

Available

Indica que la interfaz se ha configurado como interfaz de Restauración de WAN secundaria y que está disponible como reserva de la interfaz primaria.

Not Present

Indica que el adaptador de la interfaz no está enchufado.

También se utiliza como estado para un dispositivo nulo. Las interfaces de repuesto se visualizan como dispositivos nulos hasta que se activan.

HW Mismatch

Indica que el tipo de adaptador configurado no coincide con el tipo de adaptador que está presente realmente en la ranura.

HW Failure

Indica que hay un error de hardware no recuperable para el hardware de la interfaz.

Diagnostics

Indica que están ejecutándose los diagnósticos de hardware.

Disable

Utilice el mandato **disable** para poner una interfaz de red o ranura fuera de línea, haciendo que la interfaz o ranura no esté disponible. Este mandato inhabilita inmediatamente la interfaz o ranura. No se le solicita confirmación y no se visualiza ningún mensaje de verificación. Si inhabilita una interfaz o una ranura con este mandato, permanece inhabilitada hasta que utilice el mandato **test** de GWCON o un mandato **reload** de OPCON para habilitarla.

Entre el número de interfaz o red o ranura como parte del mandato. Para obtener el número de interfaz o número de ranura, utilice el mandato **configuration** de GWCON.

Mandatos GWCON

Nota: Si la interfaz que está inhabilitando está configurada como una interfaz de Redireccionamiento de WAN, se le pide si desea inhabilitar cualquier pareja primaria/alternativa de Redireccionamiento de WAN que incluye esta interfaz alternativa. Si responde *sí*, se inhabilita la interfaz y ya no está disponible como reserva de una interfaz primaria. Si responde *no*, la interfaz alternativa se inhabilita pero el Redireccionamiento de WAN intentará activarla si su interfaz primaria correspondiente se desactiva. Es aconsejable inhabilitar el Redireccionamiento de WAN en una interfaz alternativa si inhabilita la interfaz para poder extraer su adaptador. Consulte las secciones La característica de redirección de WAN, Utilización de restauración de WAN y Configuración y supervisión de restauración de WAN de la publicación *Utilización y configuración de las características* para obtener información adicional.

Sintaxis:

```
disable                _interface númerointerfaz
                        _slot número ranura
```

Disk

Utilice el mandato **disk** para listar, recuperar o suprimir los archivos relacionados con el servicio del disco duro. Se pueden listar, recuperar o suprimir las siguientes categorías de archivos: APPN, Adaptador, ELS, SYSTEM u otros (los otros archivos son los que no recaen en ninguna otra categoría). Sólo se listan los archivos que se localizan realmente. Se proporciona la siguiente información para los archivos que se localizan: el nombre, el comentario que indica lo que es el archivo, el tamaño del archivo y la fecha en la que se ha creado el archivo. Para los archivos de vuelcos del sistema, se proporciona información adicional acerca de los vuelcos. Cuando se recupera o suprime un archivo, se le solicita que confirme el mandato. Para recuperar un archivo, necesitará proporcionar también la dirección IP de destino que define dónde debe enviarse el archivo y el nombre que se ha de dar al archivo cuando se grabe.

Sintaxis:

```
disk                   _list categoría
                        _retrieve categoría
                        _delete categoría
```

Las categorías son: adapter, appn, els, other, and system.

Ejemplo:

```
+disk list system
'core' Master System dump file (uncompressed)
Size: 268435456 bytes Date: Tues Apr 06 10:054:30 1999
'core0.cmp' System dump file (compressed)
Size: 11208443 bytes Date: Tues Apr 06 10:15:28 1999
'core1.cmp' System dump file (compressed)
Size: 11150344 bytes Date: Tues Apr 06 10:54:30 1999
There are 3 different files
Do you want to see the details of the compressed dumps? [No]: n
```

Enable

Utilice el mandato **Enable** para habilitar todas las interfaces de un adaptador. Realiza la misma acción que el mandato **test** (consulte la sección "Test" en la página 132) pero ejecuta la acción para cada interfaz que utiliza el adaptador de la ranura especificada.

Error

Sintaxis:

enable slot *númeroranura*

Utilice el mandato **error** para visualizar las estadísticas de errores para la red. Este mandato proporciona un grupo de contadores de errores.

Sintaxis:

error [*númerored* o *rango_de_númerored*]

Para visualizar información acerca de múltiples interfaces, especifique el *rango_de_númerored* (o una combinación de *númerored* y *rango_de_númerored*). Por ejemplo, si especifica **error 0 3 25-50**, se visualiza la información para las redes 0, 3 y 25 a 50.

Ejemplo:

error

Nt	Interface	Input Discards	Input Errors	Input Unk	Input Proto	Input Flow Drop	Output Discards	Output Errors
0	TKR/0	0	0	0	0	0	0	0
1	PPP/0	0	0	0	0	0	0	0
2	PPP/1	0	0	0	0	0	0	0

Nt Número de interfaz de red asociada con el software.

Interface

Tipo de interfaz.

Input Discards

Número de paquetes de entrada que se han eliminado aunque no se hubiesen detectado errores para impedir que se entregasen a un protocolo de capa superior. Los paquetes pueden haberse eliminado para liberar espacio de almacenamiento intermedio.

Input Errors

Número de paquetes que se han encontrado defectuosos en el enlace de datos.

Input Unk Proto

Número de paquetes recibidos para un protocolo desconocido.

Input Flow Drop

Número de paquetes recibidos cuyo flujo se controla en la salida.

Output Discards

Número de paquetes que el dispositivo ha elegido para su eliminación en lugar de transmitirlos debido al control de flujo.

Output Errors

Número de errores de salida como, por ejemplo, los intentos de envío a través de una red que está desactivada o a través de una red que se ha desactivado durante la transmisión.

Nota: La suma de los paquetes de salida eliminados no es igual a las eliminaciones de flujo de entrada de todas las redes. La salida eliminada puede indicar paquetes originados localmente.

Mandatos GWCON

Event

Utilice el mandato **event** para acceder al entorno de consola del Sistema de anotación cronológica de sucesos (ELS). Este entorno se utiliza para configurar los filtros de mensajes temporales para la resolución de problemas. Todos los cambios realizados en el entorno de consola ELS surtirán efecto inmediatamente, pero desaparecerán cuando se reinicie el dispositivo. Consulte la sección “Capítulo 10. Utilización del Sistema de anotación cronológica de sucesos (ELS)” en la página 137 para obtener información acerca del Sistema de anotación cronológica de sucesos y sus mandatos. Utilice el mandato **exit** para volver al proceso GWCON.

Sintaxis:

event

Feature

Utilice el mandato **feature** para acceder a los mandatos de consola para características específicas del 2216 fuera de los procesos de consola de protocolo y de interfaz de red.

Entre un signo de interrogación después del mandato **feature** para obtener un listado de las características disponibles para el release de software.

Para acceder al indicador de consola de la característica, entre el mandato **feature** en el indicador GWCON seguido del número de característica o el nombre corto. La Tabla 9 en la página 97 lista los números y nombres de las características disponibles.

Una vez acceda al indicador de esa característica, puede empezar a entrar mandatos específicos para supervisar esa característica. Para volver al indicador GWCON, entre el mandato **exit** en el indicador de consola de la característica.

Sintaxis:

feature *númerocaracterística o nombre-corto-característica*

Interface

Utilice el mandato **interface** para visualizar la información de estadísticas acerca de las interfaces de red (por ejemplo, Ethernet). Este mandato puede utilizarse sin ningún calificador para proporcionar un resumen de todas las interfaces o con un calificador para revelar información detallada acerca de una interfaz específica.

Las descripciones de salida detallada para cada tipo de interfaz se proporcionan en los capítulos de *Supervisión* de la interfaz específica de esta guía. Para obtener el número de interfaz, utilice el mandato **configuration** de GWCON.

Sintaxis:

interface *[númerointerfaz o rango_de_númerointerfaz]*

Para visualizar información acerca de múltiples interfaces, especifique el *rango_de_númerored* (o una combinación de *númerointerfaz* y *rango_de_númerointerfaz*). Por ejemplo, la especificación de **interface 0 3 25-50** visualiza información para las redes 0, 3 y 25 a 50.

Ejemplo: interface

Mandatos GWCON

Nt	Nt'	Interface	Slot-Port	Self-Test Passed	Self-Test Failed	Maintenance Failed
0	0	TKR/0	Slot: 1 Port: 1	1	0	0
1	1	TKR/1	Slot: 1 Port: 2	2	1	0
2	2	TKR/2	Slot: 2 Port: 1	2	1	0
3	3	TKR/3	Slot: 2 Port: 2	2	1	0
4	4	Eth/0	Slot: 4 Port: 1	1	0	0
5	5	Eth/1	Slot: 4 Port: 2	1	0	0
6	6	Eth/2	Slot: 5 Port: 1	1	0	0
7	7	Eth/3	Slot: 5 Port: 2	3	2	2
8	8	Eth/4	Slot: 6 Port: 1	1	0	0
9	9	Eth/5	Slot: 6 Port: 2	5	4	1
10	10	FR/0	Slot: 8 Port: 0	2	1	0
11	11	X25/0	Slot: 8 Port: 1	1	0	0
12	12	PPP/0	Slot: 8 Port: 2	2	1	0
13	13	PPP/1	Slot: 8 Port: 3	1	0	0
14	14	PPP/2	Slot: 8 Port: 4	1	0	0
15	15	PPP/3	Slot: 8 Port: 5	1	0	0

Nota: Puede visualizarse la información siguiente. La pantalla varía dependiendo del dispositivo.

Nt Número de interfaz global.

Nt' Reservado para la utilización de circuito de marcación. El número de la interfaz física de red que el circuito de marcación utiliza.

Interface

Nombre de interfaz.

Slot-Port

Número de ranura y número de puerto de la interfaz.

Self-Test Passed

Número de veces que la autoprueba ha sido satisfactoria (el estado de la interfaz cambia de desactivada a activada).

Self-Test Failed

Número de veces que ha fallado la autoprueba (el estado de la interfaz cambia de activada a desactivada).

Maintenance Failed

Número de anomalías de mantenimiento.

Memory

Utilice el mandato **memory** para visualizar el uso de memoria de CPU actual en bytes, el número de almacenamientos intermedios y los tamaños de paquetes.

Para utilizar este mandato, debe haber memoria libre disponible. El número de almacenamientos intermedios de paquetes libres puede bajar a cero, dando como resultado la pérdida de algunos paquetes de entrada; sin embargo, no afecta negativamente a las operaciones del dispositivo. El número de almacenamientos intermedios libres debe permanecer constante cuando el dispositivo está desocupado. Si no lo hace, póngase en contacto con el servicio técnico.

Sintaxis:

memory

Ejemplo:

```
memory
Physical installed memory:      16 MB
Total routing (heap) memory:   12 MB
Routing memory in use:         13 %
```

```
Total Reserve Never Perm Temp Prev
```

Mandatos GWCON

			Alloc	Alloc	Alloc	Alloc
Heap memory	12231155	26488	10687312	1438487	104924	432

Number of global buffers: Total = 300, Free = 300, Fair = 77, Low = 60
Global buff size: Data = 2048, Hdr = 17, Wrap = 72, Trail = 65, Total = 2208

Physical installed memory

La cantidad total de RAM física instalada en el dispositivo.

Total routing memory

La cantidad de memoria disponible para la función de direccionamiento, sin incluir la asignada al sistema operativo base, a las extensiones del sistema ni a las opciones como, por ejemplo, APPN. Esto también se llama memoria de "almacenamiento dinámico" y coincide con el tamaño de memoria de almacenamiento dinámico "Total" proporcionado en bytes poco después.

Routing memory in use

El porcentaje de memoria total de direccionamiento que la función de direccionamiento utiliza actualmente. La memoria de almacenamiento dinámico en uso actualmente se cuenta bajo las cabeceras **Perm Alloc** y **Temp Alloc**.

Heap memory:

Cantidad de memoria utilizada para asignar dinámicamente las estructuras de datos.

Total Cantidad total de espacio disponible para asignar memoria.

Reserve

Cantidad mínima de memoria que necesitan los protocolos y características configurados actualmente.

Never Alloc

Memoria que no se ha asignado nunca.

Perm Alloc

Memoria pedida permanentemente por tareas de dispositivo.

Temp Alloc

Memoria asignada temporalmente a las tareas de dispositivo.

Prev Alloc

Memoria asignada temporalmente y devuelta.

Number of global buffers:

Total Número total de almacenamientos intermedios globales del sistema.

Free Número de almacenamientos globales disponibles.

Fair Número equitativo de almacenamientos intermedios para cada interfaz. (Consulte "Low".)

Low El número de almacenamientos intermedios libres en el que cambia la estrategia de asignación para conservar almacenamientos intermedios. Si el valor de *Free* es menor que *Low*, no se colocarán almacenamientos intermedios en ninguna cola que tenga más del número *Fair* de almacenamientos intermedios en ella.

Global buff size:

Tamaño de almacenamiento intermedio global.

Data Tamaño máximo de paquete de enlace de datos de cualquier interfaz.

Header

Suma del número máximo de cabeceras de hardware, MAC y de enlace de datos.

Wrap

Permiso otorgado para las cabeceras de capa MAC, LLC o red debido al reinicio del protocolo.

Trailer

Suma de las colas más grandes MAC y de hardware.

Total

Tamaño global de cada almacenamiento intermedio de paquetes

Network

Utilice el mandato **network** para entrar en el entorno de consola para redes soportadas como, por ejemplo, redes X.25. Este mandato obtiene el indicador de consola para la interfaz especificada. En el indicador, puede visualizar información de estadísticas como, por ejemplo, los campos de información de direccionamiento para Redes en Anillo.

Sintaxis:

```
network númerointerfaz
```

En el indicador GWCON (+), entre el mandato **configuration** para ver los protocolos y las redes para los que está configurado el dispositivo. Consulte la sección "Configuration" en la página 120 para obtener más información sobre el mandato configuration.

Entre **interface** en el indicador + para visualizar las redes para las que el dispositivo está configurado.

Entre el mandato **network** de GWCON y el número de la interfaz que desea supervisar o cambiar. Por ejemplo:

```
+network 3
X.25>
```

En el ejemplo, se visualiza el indicador X.25>. Puede visualizar información acerca de la interfaz X.25 entrando los mandatos operativos de X.25.

Después de identificar el número de la interfaz que desea supervisar, para ver información específica de la interfaz, consulte el capítulo de supervisión de este manual correspondiente a la red especificada o la interfaz de capa de enlace. Se proporciona soporte de consola para las siguientes interfaces de red y de capa de enlace:

- Ethernet
- Frame Relay
- PPP
- SDLC
- SDLC Relay (SRLY)
- Red en Anillo
- V.25bis
- X.25
- ATM
- RDSI
- Marcación de entrada
- PPP de múltiples enlaces (MP)
- Túnel de 2 capas

Mandatos GWCON

Performance

Utilice el mandato **performance** en el indicador GWCON para entrar en el entorno de supervisión del rendimiento. Consulte la sección “Capítulo 12. Configuración y supervisión del rendimiento” en la página 213 para obtener más información.

Protocol

Utilice el mandato **protocol** para comunicarse con el software de dispositivo que implementa los protocolos de red instalados en el dispositivo. El mandato **protocol** accede al entorno de mandatos de un protocolo. Después de entrar este mandato, aparece el indicador del protocolo especificado. En el indicador, puede entrar mandatos que son específicos de ese protocolo.

Sintaxis:

protocol *númeroprot*

Entre el número de protocolo o nombre corto como parte del mandato. Para obtener el número de protocolo o el nombre corto, entre en el entorno de mandatos de CONFIG (Config>) y, a continuación, entre el mandato **list configuration**. Consulte la sección “Acceso al proceso de configuración, CONFIG (Talk 6)” en la página 14 para obtener instrucciones de cómo acceder a Config>. Para volver a GWCON, entre **exit**.

Consulte el capítulo de supervisión correspondiente de este manual o en la publicación *Consulta de configuración y supervisión de protocolos* para obtener información sobre los mandatos de consola de un protocolo específico.

Queue

Utilice el mandato **queue** para visualizar estadísticas acerca de la longitud de las colas de entrada y de salida de las interfaces especificadas. La información acerca de las colas de entrada y salida proporcionada por el mandato queue incluye:

- El número total de almacenamientos intermedios asignados
- El valor de almacenamiento intermedio de nivel inferior
- El número de almacenamientos intermedios activos actualmente en la interfaz.

Sintaxis:

queue *númerointerfaz o rango_de_númerointerfaz*

Para visualizar información acerca de múltiples interfaces, especifique el *rango_de_númerored* (o una combinación de *númerointerfaz* y *rango_de_númerointerfaz*). Por ejemplo, si especifica **queue 0 3 25-50**, se visualiza información para las redes 0, 3 y 25 a 50.

Para visualizar información acerca de una sola interfaz, entre el número de interfaz o de red como parte del mandato. Para obtener el número de interfaz, utilice el mandato **configuration** de GWCON.

Ejemplo:

```
queue
      Input Queue      Output Queue
Nt Interface Alloc Low Curr Fair Curr
0 Eth/0      30 10 30    30  1
1 PPP/0      24  4 24     4   0
2 FR/0       24  4 24     5   0
```

Nt Número de interfaz de red asociada con el software.

Interface

Tipo de interfaz.

Input Queue:

Alloc Número de almacenamientos intermedios asignados a este dispositivo.

Low El umbral mínimo para almacenamientos intermedios de recepción (entrada) se utiliza para activar el control de flujo para este dispositivo. El umbral mínimo se puede configurar utilizando el mandato **set input-low-water** de CONFIG (Talk 6).

Curr El número actual de almacenamientos intermedios de este dispositivo. El valor será 0 si el dispositivo está inhabilitado.

Output Queue:

Fair El umbral máximo para la cola de salida de la interfaz cuando el control de flujo está activado para un dispositivo de entrada.

Nota: Cuando la Reserva de ancho de banda (BRS) está configurada para las interfaces PPP y Frame Relay, se pasa por alto el valor de equidad de la salida y se utilizan las longitudes de cola configurables con BRS para determinar si debe eliminarse un paquete debido al control de flujo.

Curr Número de paquetes en espera actualmente a que se transmitan en este dispositivo. La posibilidad de elegir eliminar depende del mínimo global descrito en el mandato **memory**.

Si se recibe un paquete y el valor actual de cola de entrada es menor que el valor de umbral mínimo de cola de entrada, el paquete se someterá a control de flujo. Para los paquetes originados localmente, un paquete está sujeto al control de flujo si el número de almacenamientos intermedios globales libres es menor que el umbral mínimo para almacenamientos intermedios globales. Si un paquete sujeto a control de flujo se ha de transmitir en un dispositivo que tiene un valor actual de cola de salida mayor que el umbral máximo de cola de salida (equidad), se elimina el paquete en lugar de ponerlo en cola. Cuando se elimina un paquete debido al control de flujo, el contador de eliminaciones de salida se incrementa y se anota cronológicamente el suceso ELS GW.036 o GW.057. Si el paquete no se ha originado localmente, se incrementa el contador de eliminación de flujo de entrada para la interfaz de entrada. Los contadores de eliminaciones de salida y de flujo de entrada se visualizan mediante el mandato **error** de GWCON.

Debido a los algoritmos de planificación del dispositivo, puede que los números dinámicos de Curr (en particular Input Queue Curr) no representen totalmente los valores típicos durante el reenvío de paquetes. El código de consola sólo se ejecuta cuando se han drenado las colas de entrada. Por lo tanto, generalmente Input Queue Curr no será cero solamente cuando estos paquetes estén en espera en colas de transmisión lenta.

Reset

Utilice el mandato **reset** para inhabilitar la interfaz especificada y después, volverla a habilitar utilizando nuevos parámetros de configuración interfaz, protocolo y características. Consulte la sección "Restablecimiento de interfaces" en la página 74 para obtener más información.

Sintaxis:

reset *númerointerfaz*

Mandatos GWCON

Statistics

Utilice el mandato **statistics** para visualizar información de estadísticas acerca del software de red como, por ejemplo, la configuración de las redes del dispositivo.

Sintaxis:

statistics *númerointerfaz o rango_de_númerointerfaz*

Para visualizar información acerca de múltiples interfaces, especifique el *rango_de_númerored* (o una combinación de *númerointerfaz* y *rango_de_númerointerfaz*). Por ejemplo, la especificación de **statistics 0 3 25-50** visualiza información para las redes 0, 3 y 25 a 50.

Para visualizar información acerca de una sola interfaz, entre el número de interfaz o de red como parte del mandato. Para obtener el número de interfaz, utilice el mandato **configuration** de GWCON.

Ejemplo:

```
statistics
Nt Interface      Unicast  Multicast  Bytes      Packets      Bytes
   Pkts Rcv    Pkts Rcv    Received   Trans        Trans
0  Eth/0          137      1          8832        1068         65297
1  PPP/0           0         0           0           0             0
2  PPP/1           0         0           0           0             0
```

Nt Número de interfaz de red asociada con el software.

Interface

Tipo de interfaz.

Unicast Pkts Rcv

Número de paquetes direccionados específicamente que no son de difusión ni de multidifusión en la capa MAC.

Multicast Pkts Rcv

Número de paquetes de multidifusión o de difusión recibidos.

Bytes Received

Número de bytes recibidos en esta interfaz en la capa MAC.

Packets Trans

Número de paquetes de tipo de vertimiento único, de multidifusión o de difusión transmitidos.

Bytes Trans

Número de bytes transmitidos en la capa MAC.

Test

Utilice el mandato **test** para verificar el estado de una interfaz o para habilitar una interfaz que se ha inhabilitado previamente con el mandato **disable**. Si la interfaz está habilitada y pasa tráfico, el mandato **test** eliminará la interfaz de la red y ejecutará pruebas de autodiagnóstico en la interfaz.

Sintaxis:

test *númerointerfaz*

Nota: Para que este mandato funcione, debe entrar el nombre **completo** del mandato seguido del número de interfaz.

Entre el número de interfaz o de red como parte del mandato. Para obtener el número de interfaz, utilice el mandato **configuration** de GWCON. Por ejemplo, cuando empieza la prueba, la consola visualiza el mensaje siguiente:

```
Testing net 0 Eth/0...
```

Cuando la prueba finaliza o falla, o cuando GWCON excede el tiempo de espera (después de 30 segundos), se visualizan los siguientes mensajes posibles:

```
Testing net 0 Eth/0 ...successful
Testing net 0 Eth/0 ...failed
Testing net 0 Eth/0 ...still testing
```

Algunas interfaces pueden tardar más de 30 segundos en efectuar las pruebas.

Nota: Si la interfaz que está probando está configurada como una interfaz alternativa de Redireccionamiento de WAN, se solicita:

- Si desea habilitar las parejas primaria-alternativa de la interfaz si el Redireccionamiento de WAN está inhabilitado actualmente para la interfaz alternativa.

Si responde *sí*, se produce la misma acción que cuando se entra el mandato de redireccionamiento de WAN **t 5 enable alternate-circuit** descrito en la sección Configuración y supervisión de restauración de WAN de la publicación *Utilización y configuración de las características*.

- Si desea probar la interfaz.

Normalmente una interfaz de Redireccionamiento de WAN está inhabilitada hasta que se necesita como reserva de la interfaz primaria correspondiente. Si responde *sí*, se inicia una autoprueba para la interfaz. Si responde *no*, no se produce ninguna autoprueba.

Consulte las secciones La característica de restauración de WAN, Utilización de la restauración de WAN y Configuración y supervisión de restauración de WAN de la publicación *Utilización y configuración de las características* para obtener información adicional.

Uptime

Utilice el mandato **uptime** para visualizar las estadísticas de tiempo acerca del dispositivo, incluyendo lo siguiente:

- Número de reinicios.
- Número de anomalías conocidas.
- Si la última vez se ha vuelto a cargar o reiniciar el dispositivo.
- El tiempo transcurrido desde la última vez que se volvió a cargar.
- El tiempo transcurrido desde la última vez que se reinició.

Sintaxis:

uptime

Mandatos GWCON

Capítulo 9. El proceso de gestión de mensajes (MONITR - Talk 2)

Este capítulo explica como reunir y visualizar los mensajes. Consulte la sección “Capítulo 10. Utilización del Sistema de anotación cronológica de sucesos (ELS)” en la página 137 para obtener información acerca de ELS y los formatos de los mensajes. Consulte también la publicación *IBM Nways Guía de mensajes del sistema para el registro cronológico de sucesos* para ver una descripción de cada mensaje. Este capítulo incluye las secciones siguientes:

- “¿Qué es la gestión de mensajes (MONITR)?”
- “Mandatos que afectan a la gestión de mensajes”
- “Entrada y salida del proceso de gestión de mensajes (MONITR)”
- “Recepción de mensajes”

¿Qué es la gestión de mensajes (MONITR)?

El proceso MONITR proporciona una vista de la actividad que se realiza dentro del dispositivo y de las redes. MONITR visualiza también los mensajes de la anotación cronológica del software.

Mandatos que afectan a la gestión de mensajes

Los mandatos siguientes afectan al proceso de gestión de mensajes:

- Mandatos OPCON:
 - **divert** desvía temporalmente la salida a un dispositivo diferente.
 - **flush** hace que el software elimine los mensajes que reúne.
 - **halt** invierte la acción del mandato divert.
 - **talk** visualiza la salida de mensajes.
- El mandato **set logging disposition** de CONFIG establece el dispositivo inicial al que el software envía su salida.

Entrada y salida del proceso de gestión de mensajes (MONITR)

Para entrar en el proceso de gestión de mensajes desde OPCON entre el mandato **event** o el mandato **talk 2**.

La consola visualiza los mensajes que el software ha acumulado.

Para salir de la gestión de mensajes y volver a OPCON, entre el carácter de interceptación OPCON (el valor por omisión es **Control-P**).

Recepción de mensajes

Para recibir mensajes en la consola, entre en el proceso de gestión de mensajes, tal como se describe en la sección anterior. El software visualiza todos los mensajes que ha registrado desde la última invocación. Mientras está conectado al proceso de gestión de mensajes, visualiza todos los mensajes a medida que se reciben.

Utilice los mandatos **divert** y **halt** de OPCON para ver los mensajes de software mientras realiza otro trabajo en el dispositivo. Los dispositivos permitidos desvían la salida a TTY0 (la consola local), TTY1 o TTY2 (las consolas remotas).

Capítulo 10. Utilización del Sistema de anotación cronológica de sucesos (ELS)

Este capítulo describe el Sistema de anotación cronológica de sucesos (ELS). ELS anota cronológicamente de manera continuada todos los sucesos, filtrándolos de acuerdo a los parámetros que seleccione. Una combinación de contadores operativos y el ELS proporciona información para la supervisión del estado y la actividad del sistema. La información se divide en las secciones siguientes:

- “¿Qué es ELS?”
- “Entrada y salida del entorno de configuración ELS” en la página 138
- “Conceptos de la anotación cronológica de sucesos” en la página 138
- “Utilización de ELS” en la página 141
- “Utilización de ELS para resolver un problema” en la página 143
- “Utilización y configuración de la anotación cronológica remota ELS” en la página 145
- “Utilización de almacenamiento intermedio de mensajes ELS” en la página 153

¿Qué es ELS?

ELS es un sistema de supervisión y una parte integrante del sistema operativo del dispositivo. El ELS gestiona los mensajes anotados cronológicamente como resultado de la actividad del dispositivo. Utilice los mandatos de ELS para establecer una configuración que sólo clasifique los mensajes que considere importantes. Después, puede visualizar los mensajes en la pantalla del terminal de consola, anotarlos cronológicamente en una estación de trabajo remota o enviarlos a una estación de gestión remota utilizando la detección del Simple Network Management Protocol (SNMP).

El sistema ELS y los contadores operativos son las mejores herramientas de resolución de problemas que tiene para identificar los problemas del dispositivo. Una exploración rápida de los mensajes de sucesos le indicarán si el dispositivo tiene un problema y dónde empezar a buscarlo.

En el entorno de configuración ELS, los mandatos se utilizan para establecer una configuración por omisión. Esta configuración por omisión no surte efecto hasta que se reinicializa el dispositivo.

En ocasiones, sirve de ayuda para ver temporalmente los mensajes utilizando otros parámetros de los que se han configurado en el entorno de configuración ELS, sin tener que reinicializar el dispositivo. El entorno operativo y de supervisión de ELS se utiliza para:

- Cambiar temporalmente los valores por omisión de visualización del ELS
 - Que los cambios realizados en el entorno de consola ELS surtan efecto inmediatamente.
 - Que los cambios del entorno operativo/de supervisión no se almacenen en el almacenamiento de configuración no volátil.
- Ver información de estadísticas relativas a la utilización de la RAM dinámica por parte del ELS

Nota: Los mensajes ELS específicos se describen en la publicación *IBM Nways Guía de mensajes del sistema para el registro cronológico de sucesos*.

ELS es un subproceso al que se accede desde el proceso OPCON.

Entrada y salida del entorno de configuración ELS

El entorno de configuración ELS (disponible desde el proceso CONFIG) se caracteriza por el indicador ELS Config>. Los mandatos que se entran en este indicador crean el estado por omisión de ELS que surte efecto después de reiniciar el dispositivo. Estos mandatos se describen con mayor detalle más adelante en este capítulo.

Los mandatos de configuración que tienen un subsistema, un grupo o un suceso como parámetro se ejecutan en el orden siguiente:

- Subsistema
- Grupo
- Suceso

Para establecer una configuración básica de ELS, entre el mandato **display subsystem all standard** en el indicador ELS Config>. Este mandato configura el ELS para que visualice los mensajes de todos los subsistemas con el nivel de anotación cronológica STANDARD (es decir, todos los errores y comentarios informativos inusuales).

Nota: El dispositivo no tiene ninguna configuración ELS por omisión. Debe entrar en el entorno de configuración ELS y establecer el estado por omisión.

Para entrar en el entorno de configuración ELS desde OPCON:

1. Entre el mandato **configuration**. La consola visualiza el indicador CONFIG (Config>). Si no aparece el indicador cuando entre CONFIG, pulse **Intro**.
2. En el indicador CONFIG, entre el mandato siguiente para acceder a ELS:

```
Config> eve
```

Se visualiza en la consola el indicador de configuración ELS (ELS config>). Ahora, puede entrar los mandatos de configuración ELS.

Para salir del entorno de configuración ELS, entre el mandato **exit**.

Conceptos de la anotación cronológica de sucesos

Esta sección describe cómo se anotan cronológicamente los sucesos y cómo interpretar los mensajes. También se describen los conceptos de subsistema, número de suceso y nivel de anotación cronológica. Una gran parte de la función ELS se basa en mandatos que aceptan el subsistema, el número de suceso y el nivel de anotación cronológica como parámetros.

Causas de los sucesos

Los sucesos se producen continuamente mientras el sistema funciona. Pueden estar causados por cualquiera de las razones siguientes:

- La actividad del sistema
- Los cambios de estado
- Las peticiones de servicio
- La transmisión y recepción de datos
- Los errores de datos e internos

Cuando se produce un suceso, ELS recibe datos del sistema que identifican el origen y la naturaleza del suceso. Después ELS genera un mensaje que utiliza los datos recibidos como parte del mismo.

Interpretación de un mensaje

Esta sección describe cómo interpretar un mensaje generado por ELS. La Figura 4 muestra el contenido del mensaje.

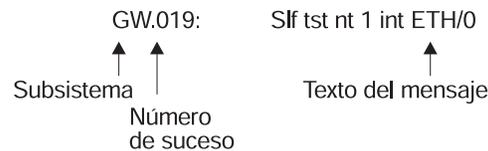


Figura 4. Mensaje generado por un suceso

La información ilustrada en la Figura 4 así como la información de nivel de anotación cronológica ELS visualizada con el mandato **list subsystem** es la siguiente:

Subsistema

Subsistema es un nombre corto predefinido para un componente de dispositivo como, por ejemplo, un protocolo o una interfaz. En la Figura 4, **GW** identifica el subsistema a través del cual se ha producido el suceso.

Otros ejemplos de subsistemas incluyen IP y ETH. En un dispositivo determinado, los subsistemas reales presentes dependen del hardware y el software configurado para ese dispositivo. Puede utilizar el mandato **list subsystem** descrito en este capítulo para ver una lista de subsistemas del dispositivo.

Entre el subsistema como parámetro para un mandato ELS cuando desee que el mandato afecte a todo el subsistema. Por ejemplo, el mandato ELS **display subsystem GW** hace que se visualicen todos los sucesos (excepto los sucesos con el nivel de anotación cronológica de 'depuración') que se producen en el subsistema GW.

Número de suceso

Número de suceso es un número predefinido, exclusivo y arbitrario asignado a cada mensaje de un subsistema. En la Figura 4, **019** es el número de suceso del subsistema GW. Puede ver una lista de todos los sucesos de un subsistema utilizando el mandato **list subsystem**, donde *subsystem* es el nombre corto para el subsistema.

El número de suceso aparece siempre con un identificador de subsistema, separado por un punto. Por ejemplo: **GW.019**. El subsistema y el número de suceso juntos identifican un suceso *individual*. Se entran como parámetros para algunos mandatos ELS. Cuando desee que un mandato sólo afecte al suceso especificado, entre el subsistema y el número de suceso como parámetro para el mandato ELS.

Nivel de anotación cronológica

El *Nivel de anotación cronológica* es un valor predefinido que clasifica cada mensaje por el tipo de suceso que lo ha generado. Utilice el mandato de consola ELS **list subsystem** para visualizar el valor del nivel de anotación cronológica. La Tabla 13 en la página 140 lista los niveles de anotación cronológica y los tipos. ERROR, INFO, TRACE, STANDARD y ALL son agregados de otros tipos de niveles de anotación cronológica. STANDARD es el valor por omisión recomendado.

Utilización de ELS

Tabla 13. Niveles de anotación cronológica

Nivel de anotación cronológica	Tipo
UI ERROR	Errores internos inusuales
CI ERROR	Errores internos comunes
UE ERROR	Errores externos inusuales
CE ERROR	Errores externos comunes
ERROR	Incluye todos los niveles de error anteriores
UINFO	Comentario informativo inusual
CINFO	Comentario informativo común
INFO	Incluye todos los niveles de comentario anteriores
STANDARD	Incluye todos los niveles de error y todos los niveles de comentario informativo (valor por omisión)
PTRACE	Por rastreo de paquete
UTRACE	Mensaje de rastreo de operación inusual
CTRACE	Mensaje de rastreo de operación común
TRACE	Incluye todos los niveles de rastreo anteriores
DEBUG	Mensaje para depuración
ALL	Incluye todos los niveles de anotación cronológica

El valor de nivel de anotación cronológica afecta al funcionamiento de los mandatos siguientes:

- **Display subsystem**
- **Nodisplay subsystem**
- **Trap subsystem**
- **Notrap subsystem**
- **Remote subsystem**
- **Noremote subsystem**

El nivel de anotación cronológica se establece para un mandato en particular cuando lo especifica como parámetro para uno de los mandatos anteriores. Por ejemplo:

```
display subsystem IP ERROR
```

La inclusión del nivel de anotación cronológica en la línea de mandatos modifica el mandato **display** de modo que siempre que se produce un suceso con el nivel de anotación cronológica UI-ERROR o CI-ERROR en el subsistema TKR, la consola visualiza el mensaje resultante.

No puede especificar el nivel de anotación cronológica para operaciones que afectan a grupos o sucesos.

Texto de mensajes

Texto de mensaje aparece en formato corto. En la Figura 4 en la página 139, S1f tst nt 1 int ETH/0 es el mensaje generado por este suceso. Las variables como, por ejemplo, *dirección_origen* o *red*, se sustituyen por datos reales cuando se visualiza el mensaje en la consola.

Algunas de las descripciones de mensajes del Sistema de anotación cronológica de sucesos hacen referencia a la variable *código_error* (normalmente precedida por rsn o reason). Indican el tipo de error de paquete detectado. La Tabla 14 en la página 141 describe los códigos de error o de terminación de paquetes. Los códigos de terminación de paquetes indican la disposición de los paquetes recibidos por el dispositivo.

Tabla 14. Códigos de terminación de paquetes (códigos de error)

Código	Significado
0	El paquete se ha puesto en cola satisfactoriamente para salida
1	Aleatorio, error no identificado
2	El paquete no se ha puesto en cola para salida debido a razones de control de flujo
3	El paquete no se ha puesto en cola porque la red está desactivada
4	El paquete no se ha puesto en cola para evitar los bucles o una mala difusión
5	El paquete no se ha puesto en cola porque el sistema principal de destino está desactivado (sólo en redes en las que se puede detectar esto)

ELS visualiza la información de red de la siguiente manera:

```
nt 1 int Eth/0 (o ) network 1, interface Eth/0,
```

donde:

- 1 es el número de red (cada red del dispositivo se numera secuencialmente a partir de cero).
- 0 es el número de unidad (las interfaces de cada tipo de hardware se numeran secuencialmente a partir de cero).

Las direcciones de hardware Ethernet y 802.5 aparecen como un número largo hexadecimal.

Las direcciones IP (Internet Protocol) se visualizan como 4 bytes decimales separados por puntos como, por ejemplo, 18.123.0.16.

Grupos

Los *grupos* son conjuntos de sucesos definidos por el usuario que reciben un nombre, el nombre del grupo. Igual que el subsistema, el subsistema y el número de suceso y el nivel de anotación cronológica, utilice el nombre del grupo como parámetro en los mandatos ELS. Sin embargo, no hay nombres de grupos predefinidos. Debe crear un grupo antes de poder especificar su nombre en la línea de mandatos.

Para crear un grupo, utilice el mandato de configuración **add**, especifique el nombre que desee para el grupo y, a continuación, especifique los sucesos que desea que formen parte del grupo. Los sucesos que añada al grupo pueden ser de distintos subsistemas y tener distintos niveles de anotación cronológica.

Después de crear un grupo, utilice el nombre de grupo para manipular los sucesos del grupo como una unidad. Por ejemplo, para desactivar la visualización de todos los mensajes de los sucesos que se han añadido a un grupo llamado grupodos, incluya el nombre del grupo en la línea de mandatos, de la manera siguiente:

```
nodisplay group grupodos
```

Para suprimir un grupo, utilice el mandato **delete**.

Utilización de ELS

Para utilizar ELS eficazmente, lleve a cabo lo siguiente:

- Sepa lo que desea antes de utilizar el sistema ELS. Defina con claridad el problema o los sucesos que desea ver antes de utilizar el proceso MONITR.

Utilización de ELS

- Ejecute el mandato **nodisplay subsystem all all** para desactivar todos los mensajes ELS.
- Active únicamente aquellos mensajes que tienen relación con el problema que está experimentando.
- Consulte la publicación *IBM Nways Guía de mensajes del sistema para el registro cronológico de sucesos* para determinar los mensajes que no son normales.

Cuando visualice inicialmente ELS desde el proceso MONITR, verá una cantidad de información considerable. Puesto que el dispositivo no puede poner en almacenamiento intermedio y visualizar todos los paquetes cuando tiene cargas de moderadas a grandes, se vacían los almacenamientos intermedios. Cuando ocurre esto se visualiza el mensaje siguiente:

```
xx messages flushed
```

El dispositivo no guarda estos mensajes. Cuando aparezca este mensaje, adapte la salida del ELS para que sólo visualice la información importante para la tarea actual que está supervisando, o utilice los mandatos avanzados de ELS para establecer un almacenamiento intermedio de mensajes. Consulte la sección “Utilización de almacenamiento intermedio de mensajes ELS” en la página 153.

Gestión de la rotación de mensajes ELS

También es importante tener en cuenta que los mensajes ELS giran de manera continuada a través de los almacenamientos intermedios del dispositivo. Para detener y reiniciar la visualización de los mensajes ELS, utilice las siguientes combinaciones de teclas:

Control-S

para detener temporalmente el desplazamiento

Control-Q

para reanudar el desplazamiento

Control-P

para volver al último proceso

También es aconsejable capturar la salida ELS en un archivo. Puede hacerlo iniciando un archivo de script o un archivo de anotaciones cronológicas desde su ubicación cuando se conecte mediante Telnet a un dispositivo. También puede hacer esto conectando un PC al puerto de consola del dispositivo e iniciando un archivo de anotaciones cronológicas desde el paquete de emulación de terminal. Esta información es necesaria para ayudar al Servicio al cliente a diagnosticar un problema.

Captura de la salida ELS utilizando una conexión Telnet en un sistema principal UNIX

Utilice una conexión Telnet en un sistema principal AIX[®] o UNIX[®] para capturar los mensajes ELS de la pantalla en un archivo del sistema principal. Antes de empezar, configure ELS para los mensajes que desea capturar utilizando los mandatos de consola ELS de la sección “Capítulo 11. Configuración y supervisión del Sistema de anotación cronológica de sucesos (ELS)” en la página 157.

Para capturar la salida ELS en un archivo de un sistema principal AIX o UNIX, siga estos pasos:

1. En el sistema principal, entre **telnet direc_ip_disp | tee nomb_arch_local**
 - *direc_ip_disp* es la dirección IP del dispositivo

- *nomb_arch_local* es el nombre del archivo del sistema principal en el que desea guardar los mensajes ELS.
 - El mandato **tee** visualiza los mensajes ELS en la pantalla y, a la vez, los copia en el archivo local.
2. En el indicador OPCON (*), entre **t 2**. Esto accede al proceso MONITR, que es el proceso que visualiza los mensajes ELS en la pantalla. Dependiendo de los mensajes ELS que haya configurado, debe ver aparecer mensajes ELS en la pantalla.

Siempre que esté en el proceso MONITR, todos los mensajes ELS se grabarán en el archivo local. Cuando salga del proceso MONITR (entrando **Control-P**) o termine la sesión Telnet, la anotación cronológica de mensajes en el archivo local se detendrá.

También puede utilizar la anotación cronológica remota en lugar de capturar la salida ELS en un sistema principal UNIX. Para obtener más información acerca de la anotación cronológica remota, consulte la sección “Utilización y configuración de la anotación cronológica remota ELS” en la página 145.

Configuración de ELS para que los mensajes de sucesos se envíen en rupturas SNMP

ELS se puede configurar para que los mensajes de sucesos se envíen a una estación de trabajo de gestión de red en una ruptura específica de la empresa SNMP. Estas rupturas son útiles para informar del estado y de los resultados de diagnóstico y a menudo se utilizan para supervisar remotamente el 2216. Cuando ELS está configurado correctamente, se generará una ruptura SNMP cada vez que se produzca el suceso seleccionado. Para obtener más información acerca de SNMP, consulte la publicación *Consulta de configuración y supervisión de protocolos*.

Para indicar a ELS que debe activarse un suceso específico para que se envíe como ruptura SNMP, escriba en el indicador ELS `config>` o en el indicador ELS>:

```
trap event ip.007
```

Nota: Si está en el indicador ELS `config>`, necesitará reemplazar.

Para habilitar la ruptura específica de la empresa ELS, siga estos pasos:

1. En el indicador SNMP `config>`, utilizando **public** como ejemplo, escriba:

```
SNMP config> add address public <network manager IP address>
SNMP config> enable trap enterprise public
SNMP config> set community access read_trap public
```

Nota: Es necesario reemplazar para activar estos cambios.

2. Habilite la estación de gestión de red para que reciba y visualice correctamente las rupturas específicas de la empresa.

Siga estos pasos para detectar grupos, subsistemas y sucesos.

Utilización de ELS para resolver un problema

Si está intentando resolver un problema en particular, visualice los mensajes relacionados con el problema. Por ejemplo, si experimenta un problema con el puente, active los mensajes de puente:

```
display subsystem srt all
display subsystem br all
```

Utilización de ELS

Inicialmente, debido al ritmo rápido con que se desplazan los mensajes en la pantalla, es aconsejable anotar los números que vea y consultarlos en el manual *Guía de mensajes del sistema para el registro cronológico de sucesos*. Cuando se haya familiarizado con los diferentes tipos de mensajes que se visualizan para un protocolo en particular, puede activar y desactivar únicamente aquellos mensajes que contienen información que necesita para solucionar un problema. Las secciones siguientes listan ejemplos de ELS específicos. Recuerde que los distintos problemas pueden necesitar distintos pasos.

Ejemplo 1 de ELS

Está interesado en consultar la frecuencia de sondeo en una interfaz de Red en Anillo y en averiguar si los sondeos son satisfactorios.

```
ELS> nodisplay subsystem all all
ELS> display subsystem tkr all
Control-P
* t 2
```

Cuando los mensajes empiecen a desplazarse, busque el mensaje ELS tkr.031.

Ejemplo 2 de ELS

El puente SRB no funciona.

1. Compruebe la configuración.
2. Utilice la consola de puente GWCON para verificar que las interfaces de puente estén habilitadas.
3. Entre:

```
* t 6
config> event
ELS config> nodisplay subsystem all all
ELS config> display subsystem srb all
ELS config> exit
config> Control-P
```

4. Reinicie el subsistema de direccionamiento. Cuando se haya reiniciado el subsistema, entre lo siguiente:

```
* t 2
```

Ejemplo 3 de ELS

El direccionador no puede comunicarse con un servidor IPX en una Ethernet.

1. Entre el mandato **talk** y el PID para GWCON.

```
* talk 5
```

La consola visualiza el indicador GWCON (+). Si el indicador no aparece cuando entre en GWCON, pulse **Intro**.

2. En el indicador GWCON (+), entre **IPX** para acceder al indicador de consola IPX (IPX>).
3. En el indicador de consola IPX, entre el mandato **slist** para verificar que se lista el servidor. (Consulte la sección sobre la supervisión de IPX en la publicación *Consulta de configuración y supervisión de protocolos* para obtener más información sobre el mandato **slist**.)
4. Compruebe la configuración IPX.
5. Entre lo siguiente:

```
* t 5
+ event
ELS> nodisplay subsystem all all
```

```

ELS> display subsystem IPX all
ELS> display subsystem eth all
ELS> Control-P
* t 2

```

Cuando los mensajes empiecen a desplazarse, busque el mensaje ELS eth.001. Esto indica que el servidor tiene un campo de tipo Ethernet incorrecto.

Utilización y configuración de la anotación cronológica remota ELS

El mensaje ELS anotado cronológicamente de forma remota contiene toda la información que está contenida en los mensajes ELS encontrados en la colas del supervisor, tal como se ve en talk 2 y contiene también información adicional, tal como aparece en la Figura 5.

Date/Time	IP address assigned by the user	Sequence Number used for detecting missing messages	Local Name assigned by the user	ELS Subsystem Name, & Formatted message
Nov 20 12:13:47	5.1.1.1	Msg [0444] from	** IBM/2216 **	:els: MPC.011 Del ent ...

Figura 5. Descripción de mensajes de la anotación cronológica del sistema

Observe las siguientes diferencias en la pantalla de anotación cronológica remota:

- El mes y el día además de la hora, que siempre se visualiza como la hora del día.
- Una dirección IP, que es la dirección IP del origen especificado por el usuario. Si un servidor DNS resuelve la dirección IP de origen en un nombre de sistema principal, se visualizará este nombre en lugar de la dirección IP.
- El dispositivo de origen añade un número de secuencia al mensaje como ayuda para la detección de mensajes eliminados. Consulte la sección “Salida de la anotación cronológica remota” en la página 149 para ver una explicación de los mensajes eliminados. Cuando el número de secuencia del mensaje alcanza 9999, el siguiente número de secuencia será 0001.
- Un “Nombre local” para el dispositivo de origen, como ayuda para distinguir entre mensajes de múltiples orígenes. Si no configura un nombre local, este campo está en blanco.

Recurso y nivel de la anotación cronológica del sistema

Los mensajes ELS anotados cronológicamente de forma remota se transmiten a través de la red en paquetes UDP con un número de puerto de destino en la cabecera UDP siempre igual a 514, el puerto de la anotación cronológica del sistema. Para recibir y procesar los paquetes UDP, el *daemon syslog daemon* (syslogd) debe estar en ejecución en la estación de trabajo remota que está recibiendo y anotando cronológicamente los mensajes ELS. Consulte la sección “Configuración de una estación de trabajo remota” en la página 146 para ver los detalles.

Aunque no se visualice en el mensaje ELS anotado cronológicamente de forma remota, cada mensaje ELS enviado en la red en un paquete UDP debe tener asignado un *recurso_anotación_cronológica_sistema* y un *nivel_anotación_cronológica_sistema*. El daemon de la anotación cronológica del sistema utiliza la combinación de recurso y nivel para determinar adónde ha de direccionar el mensaje. Normalmente, es aconsejable grabar los mensajes ELS en

Utilización de ELS

uno o varios archivos del sistema principal remoto. Otras opciones son visualizar el mensaje en la consola, enviar el mensaje a uno o varios usuarios o enviar el mensaje a otra estación de trabajo.

Los mandatos que utilice para especificar los valores de *recurso_ anotación_cronológica_sistema* y *nivel_ anotación_cronológica_sistema*, junto con otros mandatos de consola relacionados con la anotación cronológica remota, se describen en las secciones “Mandatos de supervisión ELS” en la página 180 y “Mandatos de configuración ELS” en la página 157. Revise estos mandatos antes de leer la siguiente sección.

Configuración de una estación de trabajo remota

La configuración siguiente supone que un solo 2216 está anotando cronológicamente de forma remota en una sola estación de trabajo remota. Puede configurar múltiples 2216 para que anoten cronológicamente de forma remota en la misma estación de trabajo remota. Sin embargo, un 2216 en particular sólo puede anotar cronológicamente en una sola estación de trabajo remota. El sistema operativo que se utiliza en este ejemplo es AIX 4.2. Su entorno puede diferir levemente de este. Para obtener más información sobre la anotación cronológica del sistema, consulte la documentación para el sistema operativo.

Para realizar la configuración en una estación de trabajo AIX, debe iniciar la sesión como **root**. Para configurar la estación de trabajo:

1. Cree o edite un archivo `syslog.conf` para especificar dónde se han de grabar los mensajes ELS con determinados valores de *recurso_ anotación_cronológica_sistema* y *nivel_ anotación_cronológica_sistema*. Consulte la parte final de la Figura 6 en la página 147 para ver un ejemplo de cómo especificar el destino del mensaje. Observe que debe especificarse el nombre de vía de acceso completo de los archivos de anotación cronológica. La ubicación por omisión para el archivo de configuración de la anotación cronológica del sistema es `/etc/syslog.conf`.
2. Cree los archivos para anotar cronológicamente los mensajes de la anotación cronológica del sistema que ha especificado en el archivo `syslog.conf`.
3. Inicie el daemon de la anotación cronológica del sistema entrando **syslogd**. Para iniciar el daemon de la anotación cronológica del sistema desde SRC (Controlador de recursos del sistema) entre **startsrc -s syslogd**. Si el nombre de vía de acceso del archivo de configuración no es `/etc/syslog.conf`, entre **syslogd -f nombre de vía de acceso**. Para iniciar el daemon de la anotación cronológica del sistema en modalidad de depuración, entre **syslogd -d**.

Nota: No está soportada la ejecución de múltiples instancias del daemon de anotación cronológica del sistema.

4. Si el daemon de la anotación cronológica del sistema ya está en ejecución cuando crea o modifica el archivo `syslog.conf`, debe reiniciarse para que el daemon reinicialice la configuración desde `syslog.conf`.
5. Verifique la configuración utilizando el mandato **logger** de la manera siguiente:

```
logger -p user.alert THIS IS A TEST MESSAGE (user.alert)
logger -p news.info THIS IS A TEST MESSAGE (news.info)
```

Si la configuración es correcta, se grabará `THIS IS A TEST MESSAGE ...` en los archivos especificados en `syslog.conf`.

```

# @(#)34      1.9 src/bos/etc/syslog/syslog.conf, cmdnet, bos411, 9428A410j 6/13/93 14:52:39
#
# COMPONENT_NAME: (CMDNET) Network commands.
#
# FUNCTIONS:
#
# ORIGINS: 27
#
# (C) COPYRIGHT International Business Machines Corp. 1988, 1989
# All Rights Reserved
# Licensed Materials - Property of IBM
#
# US Government Users Restricted Rights - Use, duplication or
# disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
#
# /etc/syslog.conf - control output of syslogd
#
# Each line must consist of two parts:-
#
# 1) A selector to determine the message priorities to which the
#    line applies
# 2) An action.
#
# The two fields must be separated by one or more tabs or spaces.
#
# format:
#
# <msg_src_list>          <destination>
#
# where <msg_src_list> is a semicolon separated list of <facility>.<priority>
# where:
#
# <facility> is:
#   * - all (except mark)
#   kern,user,mail,daemon, auth, syslog, lpr, news, uucp, cron, authpriv, local0 - local7
#
# <priority or level> is one of (from high to low):
#   emerg,alert,crit,err(or),warn(ing),notice,info,debug
#   (meaning all messages of this priority or higher)
#
# <destination> is:
#   /filename - log to this file
#   username[,username2...] - write to user(s)
#   @hostname - send to syslogd on this machine
#   * - send to all logged in users
#
# example:
# "mail messages, at debug or higher, go to Log file. File must exist."
# "all facilities, at debug and higher, go to console"
# "all facilities, at crit or higher, go to all users"
# mail.debug          /usr/spool/mqueue/syslog
# *.debug             /dev/console
# *.crit              *
#
#   syslog messages with facility / priority values of LOG_USER,  LOG_ALERT
user.alert           /tmp/syslog_user_alert
#
#   syslog messages with facility / priority values of LOG_NEWS,  LOG_INFO
news.info            /tmp/syslog_news_info

```

Figura 6. Archivo de configuración syslog.conf

Configuración del 2216 para la anotación cronológica remota

Para configurar un 2216:

1. En talk 6, configure el recurso de anotación cronológica remota tal como se muestra en la Figura 7 en la página 148. La dirección IP especificada como *direc-ip-origen* debe ser una dirección IP que esté configurada en el 2216 para una identificación más fácil cuando aparezca la dirección IP o el nombre de sistema principal en el mensaje ELS anotado cronológicamente de forma remota. También debe verificar que el servidor de nombres resuelva rápidamente esta dirección IP en un nombre de sistema principal o que al menos el servidor de nombres responda rápidamente con un mensaje de

Utilización de ELS

“dirección no encontrada.” Para determinar si ocurre esto, emita el mandato **host** en la estación de trabajo de la manera siguiente:

```
workstation> host 5.1.1.1  
host: address 5.1.1.1 NOT FOUND  
workstation>
```

Si la respuesta tarda más de 1 segundo, seleccione una dirección IP que se resuelva más rápidamente.

2. En talk 6 configure los sucesos y subsistemas para una anotación cronológica remota, tal como se muestra en la Figura 8 en la página 149.
3. Escriba la configuración y vuelva a cargar el dispositivo.

```
ELS config>set remote source-ip-addr 5.1.1.1  
Source IP Addr = 5.1.1.1  
  
ELS config>set remote remote-ip-addr 192.9.200.1  
Remote Log IP Addr = 192.9.200.1  
  
ELS config>set remote local-id ** IBM/2216 **  
Remote Log Local ID = ** IBM/2216 **  
  
ELS config>set remote no-msgs-in-buffer 100  
Number of messages in Remote Log Buffer must be 100-512  
Number of Messages in Remote Buffer = 100  
  
ELS config>set remote facility log_news  
Default Syslog Facility = LOG_NEWS  
  
ELS config>set remote level log_info  
Default Syslog Level = LOG_INFO  
  
ELS config>set remote on  
Remote Logging is ON  
  
ELS config>list remote  
  
----- Remote Log Status -----  
  
Remote Logging is ON  
Source IP Address = 5.1.1.1  
Remote Log IP Address = 192.9.200.1  
Default Syslog Facility = LOG_NEWS  
Default Syslog Priority Level = LOG_INFO  
Number of Messages in Remote Log = 100  
Remote Logging Local ID = ** IBM / 2216 **  
ELS config>
```

Figura 7. Configuración del 2216 para la anotación cronológica remota

```

ELS config>display sub snmp all
ELS config>remote sub snmp all log_news log_info

ELS config>display event srt.017
ELS config>remote event srt.017 log_news log_info

ELS config>display event stp.016
ELS config>remote event stp.016 log_user log_info

ELS config>display event stp.026
ELS config>remote event stp.026 log_news log_info

ELS config>display event stp.024
ELS config>remote event stp.024 log_news log_info

ELS config>display event ip.068
ELS config>remote event ip.068 log_news log_info

ELS config>display event ip.058
ELS config>remote event ip.058 log_news log_info

ELS config>display event ip.022
ELS config>remote event ip.022 log_news log_info

ELS config>display event gw.022
ELS config>remote event gw.22 log_news log_info

ELS config>display event arp.011
ELS config>remote event arp.011 log_user log_alert

ELS config>display event arp.002
ELS config>remote event arp.022 log_user log_alert

ELS config>list status
Subsystem: SNMP
Disp levels: ERROR INFO TRACE
Trap levels: none
Trace levels: none
Remote levels: ERROR INFO TRACE
Syslog Facility/Level: LOG_NEWS LOG_INFO

Event   Display Trap   Trace   Remote
SRT.017 On      Unset   Unset   On
        Syslog Facility/Level: LOG_NEWS LOG_INFO
STP.016 On      Unset   Unset   On
        Syslog Facility/Level: LOG_NEWS LOG_INFO
STP.026 On      Unset   Unset   On
        Syslog Facility/Level: LOG_NEWS LOG_INFO
STP.024 On      Unset   Unset   On
        Syslog Facility/Level: LOG_NEWS LOG_INFO
IP.068  On      Unset   Unset   On
        Syslog Facility/Level: LOG_NEWS LOG_INFO
IP.058  On      Unset   Unset   On
        Syslog Facility/Level: LOG_NEWS LOG_INFO
IP.022  On      Unset   Unset   On
        Syslog Facility/Level: LOG_NEWS LOG_INFO
GW.022  On      Unset   Unset   On
        Syslog Facility/Level: LOG_NEWS LOG_INFO
ARP.011 On      Unset   Unset   On
        Syslog Facility/Level: LOG_USER LOG_ALERT
ARP.002 On      Unset   Unset   On
        Syslog Facility/Level: LOG_USER LOG_ALERT

```

Figura 8. Configuración de subsistemas y sucesos para la anotación cronológica remota

Salida de la anotación cronológica remota

La Figura 9 en la página 150 muestra un ejemplo del archivo /tmp/syslog_news_info. Observe que el primer mensaje tiene el número de secuencia 310. Esto significa que los 309 primeros mensajes ELS no se han enviado desde el 2216 de origen. Existen varias razones para que esto ocurra:

- El recurso de anotación cronológica remota no había completado la inicialización cuando se han pasado los mensajes a ELS

Utilización de ELS

- Una ruta desde el 2216 de origen a la estación de trabajo remota no estaba en la tabla de direccionamiento
- La interfaz para el paquete UDP de salida que contiene los mensajes ELS no estaba en estado “Activada”

Observe en **1** que los mensajes 311-313 no se han anotado cronológicamente de forma remota. Esto es debido a que estaba pendiente una petición ARP y hasta que se recibe la respuesta ARP, se eliminan todos los paquetes excepto el primero, en el 2216 de origen. Además, la antememoria ARP se borra a una cadencia de refresco configurada por el usuario y se emite una nueva petición ARP. Para determinar cuándo ocurre esto, puede anotar cronológicamente de forma remota los sucesos ARP.002 y ARP.011 además de los sucesos ELS primarios de interés. La Figura 11 en la página 151 muestra los sucesos ARP anotados cronológicamente en el archivo *syslog_user_alert* que cuentan para los sucesos 445 y 446, que se indica que faltan en la Figura 9.

```
Nov 20 12:03:16 worksta01 root: ESTE ES UN MENSAJE DE PRUEBA (news.info)
Nov 20 12:08:48 5.1.1.1 Msg [0310] from ** IBM / 2216 **: els: IP.022: add nt 192.9.200.0 int 192.9.200.20
nt 0 int Eth/0
```

1 (messages 311, 312, and 313 did not get remote-logged due to ARP request outstanding - see explanation in the text)

2 (messages 314 and 315 were logged to a separate file - see explanation in the text)

```
Nov 20 12:08:48 5.1.1.1 Msg [0316] from ** IBM / 2216 **: els: IP.068: routing cache cleared
Nov 20 12:08:48 5.1.1.1 Msg [0317] from ** IBM / 2216 **: els: IP.022: add nt 5.0.0.0 int 5.1.1.1 nt 5 int Eth/4
Nov 20 12:08:48 5.1.1.1 Msg [0318] from ** IBM / 2216 **: els: SRT.017: Enabling SRT on port 5 nt 5 int Eth/4
```

(message 319 was logged to a separate file)

```
Nov 20 12:08:48 5.1.1.1 Msg [0320] from ** IBM / 2216 **: els: IP.068: routing cache cleared
```

(120 messages not shown)

```
Nov 20 12:13:33 5.1.1.1 Msg [0441] from ** IBM / 2216 **: els: GW.022: Nt fld slf tst nt 3 int Eth/3
Nov 20 12:13:33 5.1.1.1 Msg [0442] from ** IBM / 2216 **: els: GW.022: Nt fld slf tst nt 6 int Eth/5
Nov 20 12:13:38 5.1.1.1 Msg [0443] from ** IBM / 2216 **: els: GW.022: Nt fld slf tst nt 11 int ISDN/0
```

(messages 444 and 447 were logged to a separate file)

(messages 445 and 446 did not get remote-logged due to ARP request outstanding)

```
Nov 20 12:13:50 5.1.1.1 Msg [0448] from ** IBM / 2216 **: els: GW.022: Nt fld slf tst nt 4 int PPP/0
Nov 20 12:13:50 5.1.1.1 Msg [0449] from ** IBM / 2216 **: els: IP.068: routing cache cleared
Nov 20 12:13:50 5.1.1.1 Msg [0450] from ** IBM / 2216 **: els: IP.058: del nt 4.0.0.0 rt via 0.0.0.4 nt 4 int PPP/0
```

Figura 9. Contenido de ejemplo desde el archivo de información de noticias de la anotación cronológica del sistema

Si los mensajes ELS iniciales que se generan durante e inmediatamente después del arranque son de interés especial, se recomienda visualizar también estos mensajes en la cola del supervisor, que se visualiza con talk 2. La Figura 10 en la página 151 muestra la salida de talk 2 incluyendo los mensajes iniciales que no se han anotado cronológicamente de forma remota. Observe que hay un mensaje en la salida de talk 2 que indica que el recurso de anotación cronológica remota está disponible. Esto no indica que exista una ruta para la estación de trabajo remota, ni que la interfaz asociada esté en el estado “Activada”. Simplemente proporciona un punto de referencia antes del cual no se puede anotar cronológicamente de forma remota y satisfactoria ningún mensaje.

Observe también que puede contar los mensajes que faltaban (indicados en la Figura 9 por **2**) en la salida de talk 2.

```

12:08:17 SNMP.024: generic trc (P2) at snmp_mg.c(766): Now 0 trap destinations
12:08:17 SNMP.012: comm public added
12:08:17 SNMP.012: comm public added
12:08:27 SNMP.022: ext err (Z1) at snmp_resconf.c(322): add_device_if_info(): sr
rdrec failed

12:08:27 SNMP.022: ext err (Z1) at snmp_resconf.c(322): add_device_if_info(): sr
rdrec failed

12:08:27 SNMP.028: err (E2) at snmp_moh.c(1583) : Duplicate
12:08:27 SNMP.028: err (E2) at snmp_moh.c(1583) : Duplicate
12:08:28 GW.022: Nt fld slf tst nt 13 int PPP/3
12:08:28 IP.022: add nt 4.0.0.0 int 4.1.1.1 nt 4 int PPP/0

    ( 297 messages not shown )

12:08:43 GW.022: Nt fld slf tst nt 12 int PPP/2
12:08:43 GW.022: Nt fld slf tst nt 13 int PPP/3
12:08:48 IP.022: add nt 192.9.200.0 int 192.9.200.20 nt 0 int Eth/0
12:08:48 SRT.017: Enabling SRT on port 1 nt 0 int Eth/0
12:08:48 STP.016: Select as root TB-1, det topol chg
12:08:48 STP.026: Root TB-1, strt hello tmr
12:08:48 ARP.002: Pkt in 1 1 800 nt 0 int Eth/0
12:08:48 ARP.002: Pkt in 2 1 800 nt 0 int Eth/0
12:08:48 IP.068: routing cache cleared

    ( 126 messages not shown )

12:13:38 GW.022: Nt fld slf tst nt 11 int ISDN/0
12:13:47 ARP.011: Del ent 1 3 nt 0 int Eth/0
12:13:47 ARP.011: Del ent 1 3 nt 0 int Eth/0
12:13:47 ARP.002: Pkt in 1 1 800 nt 5 int Eth/4
12:13:47 ARP.002: Pkt in 2 1 800 nt 0 int Eth/0
12:13:50 GW.022: Nt fld slf tst nt 4 int PPP/0

```

Corresponding Sequence
Numbers in
Remote-Logging Files :

```

[0310] first message logged
-- not logged (ARP request) --
-- not logged (ARP request)--
-- not logged (ARP request)--
[0314]
[0315]
[0316]

[0443]
[0444]
-- not logged (ARP request) --
-- not logged (ARP request)--
[0447]
[0448]

```

Figura 10. Salida de Talk 2

Puede utilizar la indicación de la hora, que aparece en el archivo de salida de la anotación cronológica remota y en la salida de talk 2, para determinar cuándo se ha anotado cronológicamente de forma remota y satisfactoria el primer mensaje ELS. Para utilizar la indicación de la hora para ello, configure ELS de manera que la indicación de la hora de la cola del supervisor visualice la hora del día.

Observe también en la Figura 9 en la página 150 que los mensajes 311-313 no se han anotado cronológicamente de forma remota. Esto es debido a que estaba pendiente una petición ARP y hasta que se recibe la respuesta ARP, se eliminan todos los paquetes excepto el primero, en el IBM 2216 de origen. La antememoria ARP se borra a una cadencia de refresco configurada por el usuario y el dispositivo emite una nueva petición ARP. Para determinar cuándo se producen peticiones ARP, pueden anotarse cronológicamente de forma remota los sucesos ARP.002 y ARP.011, además de los sucesos ELS de interés. La Figura 11 muestra los sucesos ARP anotados cronológicamente en el archivo *syslog_user_alert* que cuentan para los sucesos 445 y 446, que se indica que faltan en la Figura 9 en la página 150.

```

Nov 20 12:02:53 worksta01 root: ESTE ES UN MENSAJE DE PRUEBA (user.alert)
Nov 20 12:08:48 5.1.1.1 Msg [0314] from ** IBM / 2216 **: els: ARP.002: Pkt in 1 1 800 nt 0 int Eth/0
Nov 20 12:08:48 5.1.1.1 Msg [0315] from ** IBM / 2216 **: els: ARP.002: Pkt in 2 1 800 nt 0 int Eth/0
Nov 20 12:08:48 5.1.1.1 Msg [0319] from ** IBM / 2216 **: els: ARP.002: Pkt in 2 1 800 nt 0 int Eth/0
Nov 20 12:13:47 5.1.1.1 Msg [0444] from ** IBM / 2216 **: els: ARP.011: Del ent 1 3 nt 0 int Eth/0
Nov 20 12:13:47 5.1.1.1 Msg [0447] from ** IBM / 2216 **: els: ARP.002: Pkt in 2 1 800 nt 0 int Eth/0

```

Figura 11. Ejemplo del contenido del archivo *Syslog_user_alert*

Puede evitar la pérdida de mensajes ELS provocada por esta secuencia ARP estableciendo una relación estática entre la dirección IP y la dirección MAC. Los pasos básicos se perfilan y se ilustran en la Figura 12 en la página 152.

1. En talk 5, ejecute “ping” para la dirección IP de la estación de trabajo remota
2. En talk 5, determine el número de interfaz (red) utilizado para enviar mensajes a la dirección IP de la estación de trabajo remota

Utilización de ELS

3. Utilice el número de red del paso anterior para determinar la dirección MAC asociada
4. En talk 6, añada una entrada ARP para establecer una relación estática entre la dirección IP y la dirección MAC

```
*t 5
+p ip

IP>ping 192.9.200.1
PING 192.9.200.20 -> 192.9.200.1: 56 data bytes, ttl=64, every 1 sec.
56 data bytes from 192.9.200.1: icmp_seq=0. ttl=64. time=0. ms
----192.9.200.1 PING Statistics----
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0/0/0 ms

IP>dump

  Type  Dest net          Mask          Cost   Age      Next hop(s)
  .
  Dir*  192.9.200.0      FFFFFFF0      1      102305   Eth/0
  .

IP>exit
+int

Net  Net'  Interface  Slot-Port          Self-Test  Self-Test  Maintenance
0    0     Eth/0      Slot: 1  Port: 1          Passed     Failed     Failed
                                1          0            0
  .

+p arp
ARP>dump
Network number to dump [0]? 0
Hardware Address      IP Address      Refresh
02-60-8C-2D-69-5D    192.9.200.1    2

Control-P
*t 6
config>p arp
ARP config>add entry
Interface Number [0]? 0
Protocol [IP]? IP
IP Address [0.0.0.0]? 192.9.200.1
Mac Address []? 02608C2D695D
ARP config> list entry

Mac address translation configuration

IF #      Prot #  Protocol -> Mac address
0         0      192.9.200.1 -> 02608C2D695D
ARP config>exit
Config>write

Control-P
*reload
Are you sure you want to reload the gateway? (Yes or [No]): Yes
(after reload, static ARP entry is active)
```

Figura 12. Ejemplo de configuración de una entrada ARP estática

Consideraciones adicionales

Mensajes ELS que contienen direcciones IP

Los mensajes ELS que contienen una dirección IP que coincide con la dirección IP de la estación de trabajo remota no se anotarán cronológicamente de forma remota, incluso si se configuran para ello, y pueden aparecer bajo talk 2. Estos mensajes se eliminan en lugar de anotarse cronológicamente de forma remota para evitar enviar demasiados paquetes UDP en la red.

Anotación cronológica duplicada

Si se repite el valor de un recurso en *syslog.conf*, por ejemplo:

```
user.debug      /tmp/syslog_user_debug
user.alert      /tmp/syslog_user_alert
```

El daemon de anotación cronológica del sistema sólo anotará cronológicamente mensajes `user.debug` en el archivo `/tmp/syslog_user_debug` mientras que los mensajes `user.alert` se anotarán cronológicamente en el archivo `/tmp/syslog_user_debug` y el archivo `/tmp/syslog_user_alert`. Esto es coherente con el diseño de la anotación cronológica del sistema que anota cronológicamente las condiciones más graves en múltiples lugares.

Para evitar esta anotación cronológica duplicada, se recomienda especificar diferentes valores de recursos en el archivo `syslog.conf`. Están disponibles un total de 19 valores de recursos.

Números de secuencia repetidos en los archivos de salida de la anotación cronológica del sistema

Dependiendo de la configuración de la red, es posible duplicar paquetes UDP que contienen mensajes ELS para el sistema principal remoto. También es posible que los paquetes lleguen en orden diferente del que se han transmitido. Un ejemplo de este fenómeno se muestra en la Figura 13. Observe que los mensajes con los números de secuencia 628 a 633 se anotan cronológicamente dos veces. Observe también que después de la primera aparición del número de secuencia 0630, aparece otra vez el número de secuencia 0629 seguido de la segunda aparición de 0630.

```
Apr 01 10:48:33 0.0.0.0 Msg [0628] from: RA22: : els: IPX.018: SAP gen rply sent nt 5 int TKR/1, 1 pkts
Apr 01 10:48:33 0.0.0.0 Msg [0628] from: RA22: : els: IPX.018: SAP gen rply sent nt 5 int TKR/1, 1 pkts
Apr 01 10:49:08 0.0.0.0 Msg [0629] from: RA22: : els: IPX.037: RIP resp sent nt 0 int TKR/0, 1 pkts
Apr 01 10:49:08 0.0.0.0 Msg [0630] from: RA22: : els: IPX.018: SAP gen rply sent nt 0 int TKR/0, 1 pkts
Apr 01 10:49:08 0.0.0.0 Msg [0629] from: RA22: : els: IPX.037: RIP resp sent nt 0 int TKR/0, 1 pkts
Apr 01 10:49:08 0.0.0.0 Msg [0630] from: RA22: : els: IPX.018: SAP gen rply sent nt 0 int TKR/0, 1 pkts
Apr 01 10:49:33 0.0.0.0 Msg [0631] from: RA22: : els: IPX.037: RIP resp sent nt 5 int TKR/1, 1 pkts
Apr 01 10:49:33 0.0.0.0 Msg [0631] from: RA22: : els: IPX.037: RIP resp sent nt 5 int TKR/1, 1 pkts
Apr 01 10:49:33 0.0.0.0 Msg [0632] from: RA22: : els: IPX.018: SAP gen rply sent nt 5 int TKR/1, 1 pkts
Apr 01 10:49:33 0.0.0.0 Msg [0632] from: RA22: : els: IPX.018: SAP gen rply sent nt 5 int TKR/1, 1 pkts
Apr 01 10:50:08 0.0.0.0 Msg [0633] from: RA22: : els: IPX.037: RIP resp sent nt 0 int TKR/0, 1 pkts
Apr 01 10:50:08 0.0.0.0 Msg [0633] from: RA22: : els: IPX.037: RIP resp sent nt 0 int TKR/0, 1 pkts
```

Figura 13. Ejemplo de números de secuencia repetidos en la salida de la anotación cronológica del sistema

Puesto que ni la anotación cronológica del sistema ni UDP tienen la posibilidad de manejar paquetes duplicados o fuera de secuencia, es importante reconocer la posibilidad de que se produzcan números de secuencia duplicados.

Utilización de almacenamiento intermedio de mensajes ELS

El almacenamiento intermedio de mensajes es una característica avanzada de ELS que puede ayudarle en la determinación de problemas. Puede configurar valores por omisión que ELS utilizará para el almacenamiento intermedio de mensajes o cambiar la forma en que se almacenan los mensajes mientras el dispositivo está en funcionamiento. El almacenamiento intermedio de mensajes puede minimizar la pérdida de información debido al reinicio de los mensajes en los almacenamientos intermedios de mensajes por omisión. Se puede acceder al almacenamiento intermedio de mensajes a través del mandato de configuración o de supervisión **advanced**. Le permite:

- Especificar si está activo el almacenamiento intermedio.

Utilización de ELS

- Especificar los sucesos que se graban en el almacenamiento intermedio de mensajes.
- Detener el almacenamiento intermedio y liberar la memoria asignada para ello.
- Visualizar el estado del almacenamiento intermedio de mensajes.
- Especificar un suceso que detenga el almacenamiento intermedio de mensajes y la acción que el sistema efectúa cuando se produce el suceso.
- Enviar una versión formateada del almacenamiento intermedio a un archivo de un servidor remoto.
- Ver un número específico o todos los mensajes ELS del almacenamiento intermedio.
- Grabar el almacenamiento intermedio en una unidad de disco duro si está presente una unidad de disco duro.
- Leer un archivo que contiene un almacenamiento intermedio de mensajes ELS formateado desde la unidad de disco duro, si está presente una unidad de disco duro.
- Enviar un archivo que contenga un almacenamiento intermedio de mensajes ELS formateado desde la unidad de disco duro, si está presente una unidad de disco duro.

Para los detalles de los mandatos, consulte las secciones “Mandatos de configuración de almacenamiento intermedio de mensajes ELS” en la página 176 y “Mandatos de la supervisión de almacenamientos intermedios de mensajes ELS” en la página 206.

El ejemplo siguiente muestra cómo configurar el almacenamiento intermedio de mensajes ELS.

Nota: El establecimiento del tamaño de almacenamiento intermedio de ELS avanzado debe realizarse bajo talk 6. El resto de pasos de configuración pueden realizarse bajo talk 5 o talk 6.

```
*t 6
Gateway user configuration
Config>event
Event Logging System user configuration
ELS config>advanced
Advanced ELS Config Console
ELS Config Advanced>set buffer
Enter buffer size in range 0 to 15219 KB [5073]?
Buffer size set to 5073 KB
NOTE: Any more config changes made before rebooting
could affect the availability of sufficient memory after
reboot!
ELS Config Advanced>exit
ELS config>exit
Config>write
Config>
*reload
Are you sure you want to reload the gateway? (Yes or [No]): Yes
```

(after reloading...)

```
*t 5

CGW Operator Console

+event
Event Logging System user console
ELS>advanced
Advanced ELS Console
ELS Advanced>list status
-----Advanced ELS Configuration-----
Logging Status: OFF Wrap Mode: ON Logging Buffer Size: 5073 KB
```

```

Stop-Event: NONE Stop-String: NONE
Additional Stop-Action: NONE
-----Run-Time Status-----
Has Stop Condition Occurred? NO Messages currently in buffer: 0

ELS Advanced>set stop event gw.26
Stop Event "GW.026" has been set
ELS Advanced>set stop string Mnt nt 5
Stop String set to "Mnt nt 5"
ELS Advanced>set stop action APPN-DUMP
Stop Action has been set to APPN-DUMP
ELS Advanced>set wrap off
Advanced Wrap Mode set to OFF.

ELS Advanced>log subsys gw all
ELS Advanced>set logging on
Advanced Logging set to ON.
ELS Advanced>list status
-----Advanced ELS Configuration-----
Logging Status: OFF Wrap Mode: OFF Logging Buffer Size: 5073 KB
Stop-Event: GW.026 Stop-String: Mnt nt 5
Additional Stop-Action: APPN-DUMP
-----Run-Time Status-----
Has Stop Condition Occurred? YES Messages currently in buffer: 2

ELS Advanced>view all noscroll

[1] 10:52:10 GW.026: Mnt nt 0 int Eth/0
[2] 10:52:10 GW.026: Mnt nt 5 int Eth/1 1

```

1 Esto ha provocado la acción de parar.

Capítulo 11. Configuración y supervisión del Sistema de anotación cronológica de sucesos (ELS)

Este capítulo describe cómo configurar los sucesos anotados cronológicamente por ELS y cómo utilizar los mandatos ELS. La información incluye las secciones siguientes:

- “Acceso al entorno de configuración ELS”
- “Mandatos de configuración ELS”
- “Entrada y salida del entorno operativo ELS” en la página 180
- “Mandatos de supervisión ELS” en la página 180

Para obtener más información sobre el Sistema de anotación cronológica de sucesos y cómo interpretar los mensajes de sucesos ELS, consulte la sección “Capítulo 10. Utilización del Sistema de anotación cronológica de sucesos (ELS)” en la página 137.

Acceso al entorno de configuración ELS

El entorno de configuración ELS se caracteriza por el indicador ELS `config>`. Los mandatos entrados en este indicador se describen en la sección “Capítulo 11. Configuración y supervisión del Sistema de anotación cronológica de sucesos (ELS)”.

Para entrar en el entorno de configuración ELS:

1. Entre **configuration**.

La supervisión visualiza el indicador `Config>`. Si no aparece el indicador, pulse **Intro**.

2. En el indicador `Config>`, entre el mandato siguiente para acceder a ELS:

`event`

La supervisión visualiza el indicador de configuración ELS (`ELS config>`). Ahora, puede entrar los mandatos de configuración ELS.

Para salir del entorno de configuración ELS, entre el mandato **exit**.

Mandatos de configuración ELS

La Tabla 15 resume los mandatos de configuración ELS. El resto de esta sección describe cada uno con detalle. Después de acceder al entorno de configuración ELS, puede entrar mandatos de configuración ELS en el indicador ELS `Config>`.

Tabla 15. Resumen de los mandatos de configuración ELS

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página 10.
Add	Añade un suceso a un grupo existente o crea un nuevo grupo.
Advanced	Le lleva al entorno de configuración avanzada, en el que puede configurar el almacenamiento intermedio de mensajes.
Clear	Borra toda la información de configuración ELS.
Default	Restablece el valor de visualización o de detección de un suceso, grupo o subsistema.

Mandatos de configuración ELS (Talk 6)

Tabla 15. Resumen de los mandatos de configuración ELS (continuación)

Mandato	Función
Delete	Suprime un número de suceso de un grupo existente o suprime todo un grupo.
Display	Habilita la visualización de los mensajes en el monitor de consola.
Filter	Filtra los mensajes ELS basándose en el número de red.
List	Lista la información sobre los valores y mensajes ELS.
Nodisplay	Inhabilita la visualización de mensajes en la consola.
Noremote	Inhabilita la anotación cronológica remota en una estación de trabajo remota.
Notrace	Controla la inhabilitación de los sucesos de rastreo de paquetes.
Notrap	Impide que se envíen los mensajes en detecciones SNMP.
Remote	Permite que los mensajes se anoten cronológicamente en una estación de trabajo remota.
Set	Establece el parámetro pin y las opciones de la característica de indicación de la hora.
Trace	Controla la habilitación de los sucesos de rastreo de paquetes.
Trap	Permite enviar los mensajes a una estación de trabajo de gestión de la red en detecciones SNMP.
View	Permite la visualización de los paquetes rastreados.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página 11.

Add

Utilice el mandato **add** para añadir un suceso individual a un grupo existente o para crear un nuevo grupo. Los nombres de grupo deben empezar por una letra y son sensibles a las mayúsculas y minúsculas. No puede añadir todo un subsistema a un grupo.

Sintaxis:

add *nombre_grupo subsistema.número_suceso*

Nota: Si no existe el grupo especificado, la siguiente solicitud le pide que confirme la creación de un nuevo grupo:

Group not found. Create new group? (yes or no)

Advanced

Utilice el mandato **advanced** para entrar en el entorno de configuración avanzada. En este entorno se configura el almacenamiento intermedio de mensajes.

Sintaxis:

advanced

Clear

Utilice el mandato **clear** para borrar toda la información de configuración ELS.

Sintaxis:

clear

Ejemplo:

`clear`

You are about to clear all ELS configuration information
Are you sure you want to do this (Yes or No):

Default

Restablece el valor de visualización o de detección de un suceso, grupo o subsistema de vuelta al estado de inhabilitado.

Sintaxis:

default display
trap
remote

display *suceso o grupo o subsistema*

Controla la salida de la pantalla de los mensajes para la supervisión.

trap *suceso o grupo o subsistema*

Controla la generación de detecciones para la estación de gestión de la red.

remote *suceso o grupo o subsistema*

Controla la generación de detecciones para la estación remota.

Delete

Utilice el mandato **delete** para suprimir un número de suceso de un grupo existente o para suprimir todo el grupo. Si el suceso especificado es el último de un grupo, se le notificará. Si se ha especificado *todos* en lugar de *subsistema.número_suceso*, una solicitud le pide que confirme la supresión de todo el grupo.

Sintaxis:

delete *nombre_grupo subsistema.número_suceso*

Display

Utilice el mandato **display** para habilitar la visualización de mensajes en el monitor de supervisión para sucesos específicos, un rango de sucesos para un subsistema, grupos o subsistemas.

Sintaxis:

display event . . .
group . . .
range . . .
subsystem . . .

event *subsistema.númerosuceso*

Visualiza mensajes del suceso especificado (*subsistema.númerosuceso*).

group *nombregrupo*

Visualiza los mensajes para un grupo especificado (*nombregrupo*).

range *nombresubsistema número_primer_suceso número_último_suceso*

Donde *número_primer_suceso* es el número del primer suceso del rango de sucesos especificado y *número_último_suceso* es el número del último suceso del rango de sucesos especificado.

Mandatos de configuración ELS (Talk 6)

Visualiza un rango de mensajes para el subsistema especificado.

Ejemplo:

```
display range gw 19 22
```

Visualiza los sucesos gw.19, gw.20, gw.21 y gw.22.

subsystem *nombresubsistema*

Visualiza los mensajes asociados con el subsistema especificado. Para averiguar qué subsistemas están en el dispositivo, escriba **list subsystems**.

Nota: Aunque ELS soporta todos los subsistemas del dispositivo, no todos los dispositivos soportan todos los subsistemas. Consulte la publicación *Guía de mensajes del sistema para el registro cronológico de sucesos* para ver una lista de los subsistemas soportados actualmente.

Filter

Utilice el mandato **filter** para acceder al entorno de mandatos de configuración de filtros. Consulte la sección "Mandatos de configuración de filtros de red ELS" en la página 173 para ver los detalles completos de los mandatos.

Sintaxis:

```
filter net
```

List

Utilice el mandato **list** para obtener información actualizada relativa a los valores ELS y a los listados de los mensajes seleccionados.

Sintaxis:

```
list all  
filter-status  
groups  
pin  
remote-log status  
status  
subsystem . . .  
subsystems all  
trace-status
```

all Lista la información de todas las categorías de **list**.

filter-status

Lista los filtros de números de red ELS.

groups

Lista los nombres de grupos definidos por el usuario y su contenido.

pin

Lista el número actual de mensajes de sucesos ELS enviados en detecciones SNMP (por segundo).

remote-log status

Lista los valores actuales de las opciones de anotación cronológica remota.

Ejemplo:

```
list r

Remote Logging is ON
Source IP Address = 192.67.38.2
Remote Log IP Address = 192.9.200.1
Default Syslog Facility = LOG_DAEMON
Default Syslog Priority Level = LOG_CRIT
Number of Messages in Remote Log = 256
Remote Logging Local ID = MYHOSTNAME
```

status Lista los subsistemas, grupos y sucesos que se han modificado por mandatos **display**, **nodisplay**, **trap**, **notrap**, **trace**, **notrace**, **remote** y **noremove**.

Ejemplo:

```
list status

Subsystem:          TKR
Disp Levels:        STANDARD
Trap levels:         none
Trace levels:        none
Remote levels:       ERROR INFO TRACE
Syslog Facility/Level: LOG_USER LOG_INFO

Group      Disp      Trap      Trace  Remote
Mygroup    Unset    Unset    Unset   On
           Syslog Facility/Level: LOG_DAEMON LOG_CRIT

Event      Disp      Trap      Trace  Remote
IP.007     Unset    Unset    Unset   On
           Syslog Facility/Level: LOG_CRON LOG_NOTICE
```

Nota: No sólo la anotación cronológica remota está habilitada, sino que la visualización incluye los valores de Recurso/Nivel de anotación cronológica del sistema para cada subsistema, grupo y suceso. Los rangos de sucesos se listan como sucesos individuales.

subsystem

Lista los nombres sucesos y descripciones de todos los subsistemas.

(Puede encontrar un ejemplo de salida de mandato **list subsystem** en la página 184.)

subsystem *subsistema*

Lista todos los sucesos de un subsistema especificado.

Ejemplo:

```
list subsystem gw
```

Event	Level	Message
GW.001	ALWAYS	Copyright 1984 Mass Institute of Technology
GW.002	ALWAYS	Portable CGW %s Rel %s strtd
GW.003	ALWAYS	Unus pkt len %d nt %d int %s/%d
GW.004	ALWAYS	Sys %s q adv alloc %d excd %d
GW.005	ALWAYS	Bffrs: %d avail %d idle fair %d low %d
GW.006	C-INFO	Pkt frm nt %d int %s/%d for uninit prt, disc
GW.007	C-INFO	Ip err %x nt %d int %s/%d
GW.008	U-INFO	Ip ovfl nt %d int %s/%d, disc
GW.009	UI-ERROR	Nt dwn ip rstrt nt %d int %s/%d
GW.010	UI-ERROR	Ip q len %d no ip buf nt %d int %s/%d
GW.011	U-INFO	Op err %x hst %wo nt %d int %s/%d
GW.012	U-INFO	Op err cnt excd hst %wo nt %d int %s/%d
GW.013	U-INFO	Rtrns cnt excd hst %wo nt %d int %s/%d
GW.014	UI-ERROR	Nt dwn op rstrt nt %d int %s/%d
GW.015	UI-ERROR	Nt dwn to hst %wo nt %d int %s/%d
GW.016	U-INFO	Op ovfl to hst %wo nt %d int %s/%d
GW.017	UE-ERROR	Intfc hdw mssng nt %d int %s/%d
GW.018	U-TRACE	Strt nt slf tst nt %d int %s/%d
GW.019	C-INFO	Slf tst nt %d int %s/%d

Mandatos de configuración ELS (Talk 6)

```
GW.020    U-TRACE   Nt pss slf tst nt %d int %s/%d
GW.021    UE-ERROR  Nt up nt %d int %s/%d
GW.022    U-TRACE   Nt fld slf tst nt %d int %s/%d
```

subsystems all

Lista todos los sucesos de todos los subsistemas.

trace-status

Visualiza la información del estado del rastreo de paquetes, incluyendo la información de configuración y de tiempo de ejecución.

Ejemplo:

```
list trace-status
```

```
----- Configuration -----
Trace Status:ON  Wrap Mode:ON  Decode Packets:ON  HD Shadowing:ON
RAM Trace Buffer Size:100000  Maximum Trace Buffer File Size:10000000
Max Packet Bytes Trace:256  Default Packet Bytes Traced:100
Trace File Record Size:2048  Stop Trace Event: TCP.013
Maximum Hours to HD Shadow: 1
```

Nodisplay

Utilice el mandato **nodisplay** para seleccionar y desactivar la visualización de mensajes en la consola.

Sintaxis:

```
nodisplay          event. . .
                   group . . .
                   range . . .
                   subsystem . . .
```

event *subsistema.númerosuceso*

Suprime la visualización de un suceso especificado (*subsistema.númerosuceso*).

group *nombregrupo*

Suprime la visualización de los mensajes que se han añadido previamente al grupo especificado (*nombregrupo*).

range *nombresubsistema número_primer_suceso número_último_suceso*

Donde *número_primer_suceso* es el número del primer suceso del rango de sucesos especificado y *número_último_suceso* es el número del último suceso del rango de sucesos especificado.

Suprime la visualización de un rango de mensajes para el subsistema especificado.

Ejemplo:

```
nodisplay range gw 19 22
```

Suprime la visualización de los sucesos gw.19, gw.20, gw.21 y gw.22.

subsystem *nombresubsistema*

Suprime la visualización de los mensajes asociados con el subsistema especificado.

Noremote

Utilice el mandato **noremote** para suprimir la anotación cronológica de sucesos en una estación de trabajo remota basándose en el número de suceso, grupo, rango de sucesos o subsistema.

Mandatos de configuración ELS (Talk 6)

Nota: Normalmente, con el mandato **noremote**, no hay necesidad de especificar un *recurso_ anotación_cronológica_sistema* ni un *nivel_ anotación_cronológica_sistema*, como la hay con el mandato **remote**. Sin embargo, para el mandato **noremote subsystem**, existe la opción de suprimir selectivamente niveles de mensajes específicos (por ejemplo, sólo de “error” o sólo de “rastreo”) en lugar de desactivarlos todos. (Si no especifica ningún nivel de mensajes en particular, se supone “todos”). Además, con el mandato **noremote subsystem**, puede establecer un *recurso_ anotación_cronológica_sistema* y un *nivel_ anotación_cronológica_sistema* para cualquier nivel de mensajes restante que no se haya desactivado.

Sintaxis:

```
noremote          _event . . .  
                   _group . . .  
                   _range . . .  
                   _subsystem . . .
```

event *subsistema.numerosuceso*

Suprime la anotación cronológica remota de mensajes para el suceso especificado.

group *nombre.grupo*

Suprime la anotación cronológica remota de mensajes que se han añadido previamente al grupo especificado (*nombre.grupo*).

range *nombresubsistema número_primer_suceso número_último_suceso*

Donde *número_primer_suceso* es el número del primer suceso del rango de sucesos especificado y *número_último_suceso* es el número del último suceso del rango de sucesos especificado.

Suprime la anotación cronológica remota de un rango de mensajes para el subsistema especificado.

Ejemplo:

```
noremote range gw 19 22
```

Suprime la anotación cronológica remota de los sucesos gw.019, gw.020, gw.021 y gw.022

subsystem *nombre.subsistema [recurso_ anotación_cronológica_sistema nivel_ anotación_cronológica_sistema]*

Suprime la anotación cronológica remota de los mensajes asociados con el subsistema especificado (*nombre.subsistema*).

Ejemplo 1:

```
noremote subsystem tkr
```

Suprime la anotación cronológica remota de todos los mensajes “tkr”.

Ejemplo 2:

```
ELS config> noremote subsystem tkr info  
ELS config> SYSLOG FACILITY[LOG_USER]?  
ELS config> SYSLOG LEVEL[LOG_INFO]?
```

En este ejemplo, “LOG_USER” y “LOG_INFO” eran los valores tomados la última vez para el subsistema TKR. El mandato especificado desactiva la anotación cronológica remota para el subsistema TKR sólo para los

Mandatos de configuración ELS (Talk 6)

mensajes codificados para "info". Puesto que no se han especificado *recurso_ anotación_cronológica_sistema* y *nivel_ anotación_cronológica_sistema*, el software solicita el *recurso_ anotación_cronológica_sistema* y el *nivel_ anotación_cronológica_sistema*. Si entra otro valor en las solicitudes, ese valor sustituirá al *recurso_ anotación_cronológica_sistema* y al *nivel_ anotación_cronológica_sistema* para el resto de mensajes anotados cronológicamente de forma remota para el subsistema TKR.

Utilice los mandatos **list all** o **list status** para visualizar lo que ha establecido con los mandatos **noremote** y **remote**.

Para obtener más información acerca del *recurso_ anotación_cronológica_sistema* y *nivel_ anotación_cronológica_sistema* consulte la sección "Remote" en la página 165.

Notrace

Inhabilita el rastreo de paquetes para el suceso/rango/subsistema/grupo especificado.

Sintaxis:

```
notrace                event . . .  
                        group . . .  
                        range . . .  
                        subsystem . . .
```

event *subsistema.numerosuceso*

Suprime el envío de datos de rastreo de paquetes para el *numerosuceso* especificado

group *nombregrupo*

Suprime el envío de datos de rastreo de paquetes que se ha añadido previamente al grupo especificado (*nombregrupo*).

range *nombresubsistema número_primer_suceso número_último_suceso*

Donde *número_primer_suceso* es el número del primer suceso del rango de sucesos especificado y *número_último_suceso* es el número del último suceso del rango de sucesos especificado.

Inhabilita el envío de datos de rastreo de paquetes para un rango de mensajes para el subsistema especificado.

Ejemplo:

```
trace range gw 19 22
```

Suprime el envío de datos de rastreo de paquetes para los sucesos gw.19, gw.20, gw.21 y gw.22.

subsystem *nombresubsistema*

Suprime el envío de datos de rastreo de paquetes para el subsistema especificado (*nombresubsistema*).

Notrap

Utilice el mandato **notrap** para seleccionar y desactivar mensajes de modo que ya no se envíen a la estación de trabajo de gestión de la red en detecciones SNMP.

Sintaxis:

notrap event . . .
 group . . .
 range . . .
 subsystem . . .

event *subsistema.númerosuceso*

Suprime el envío del mensaje especificado en una detección SNMP (*subsistema.númerosuceso*).

group *nombregrupo*

Suprime el envío de mensajes en detecciones SNMP que se han añadido previamente al grupo especificado (*nombregrupo*).

range *nombresubsistema número_primer_suceso número_último_suceso*

Donde *número_primer_suceso* es el número del primer suceso del rango de sucesos especificado y *número_último_suceso* es el número del último suceso del rango de sucesos especificado.

Suprime el envío de mensajes para los sucesos del rango especificado para el subsistema especificado en detecciones SNMP.

Ejemplo:

```
notrap range gw 19 22
```

Suprime el envío de mensajes para los sucesos gw.19, gw.20, gw.21 y gw.22 en detecciones SNMP.

subsystem *nombresubsistema*

Suprime el envío de mensajes en detecciones SNMP que están asociadas con el subsistema especificado.

Remote

Utilice el mandato **remote** para seleccionar los sucesos que se han de anotar cronológicamente en una estación de trabajo remota por número de suceso, rango de sucesos, grupo o subsistema.

Sintaxis:

remote event . . .
 range . . .
 group . . .
 subsystem . . .

event *subsistema.númerosuceso recurso_ anotación_cronológica_sistema nivel_ anotación_cronológica_sistema*

Hace que el suceso especificado se anote cronológicamente de forma remota. El daemon de anotación cronológica del sistema utiliza los valores de recurso y de nivel de anotación cronológica del sistema en la estación de trabajo remota para determinar dónde tiene que anotar cronológicamente los mensajes. Este valor prevalece sobre los valores por omisión que se establecen con los mandatos **set facility** y **set level**.

recurso_ anotación_cronológica_sistema
 log_auth

Mandatos de configuración ELS (Talk 6)

log_authpriv
log_cron
log_daemon
log_kern
log_lpr
log_mail
log_news
log_syslog
log_user
log_uucp
log_local0-7

nivel_ anotación_cronológica_sistema

log_emerg
log_alert
log_crit
log_err
log_warning
log_notice
log_info
log_debug

Estos valores NO tienen ninguna asociación particular con ningún daemon de IBM 2216. Solamente son identificadores que el daemon de anotación cronológica del sistema utiliza en la estación de trabajo remota.

range *nombresubsistema número_primer_suceso número_último_suceso*
recurso_ anotación_cronológica_sistema nivel_ anotación_cronológica_sistema

Donde *número_primer_suceso* es el número del primer suceso del rango de sucesos especificado y *número_último_suceso* es el número del último suceso del rango de sucesos especificado.

Hace que los sucesos del rango especificado para el subsistema especificado se anoten cronológicamente de forma remota basándose en los valores de *recurso_ anotación_cronológica_sistema* y *nivel_ anotación_cronológica_sistema*. Consulte “el mandato remote event” en la página 165.

Ejemplo:

```
remote range gw 19 22 log_user log_info
```

Hace que los sucesos gw.19, gw.20, gw.21 y gw.22 se anoten cronológicamente de forma remota en el valor *recurso_ anotación_cronológica_sistema* de log_user y el valor *nivel_ anotación_cronológica_sistema* de log_info.

group *grupo.nombre recurso_ anotación_cronológica_sistema*
nivel_ anotación_cronológica_sistema

Permite que los sucesos que pertenecen al grupo especificado se anoten cronológicamente de forma remota basándose en los valores de *recurso_ anotación_cronológica_sistema* y *nivel_ anotación_cronológica_sistema*. Consulte “el mandato remote event” en la página 165.

Mandatos de configuración ELS (Talk 6)

subsystem *nombre.subsistema nivel_mensaje*

recurso_ anotación_cronológica_sistema nivel_ anotación_cronológica_sistema

Donde *nombre.subsistema* es el nombre del subsistema y *nivel_mensaje* es el nivel de los mensajes seleccionados del subsistema.

Hace que los sucesos del *nombre.subsistema* especificado cuyo *nivel_mensaje* concuerde con el *nivel_mensaje* especificado, se anoten cronológicamente de forma remota en los archivos basándose en los valores de *recurso_ anotación_cronológica_sistema* y *nivel_ anotación_cronológica_sistema*. Consulte “el mandato remote event” en la página 165.

Nivel_mensaje es un valor como, por ejemplo, “ALL,” “ERROR,” “INFO” o “TRACE”. Consulte la sección “Nivel de anotación cronológica” en la página 139. El valor especificado en el mandato **remote** debe concordar con el valor codificado en el suceso en particular del subsistema, o si no el suceso del subsistema no se anotará cronológicamente de forma remota.

Ejemplo:

```
remote subsystem ETH all log_user log_info
```

En el ejemplo anterior, todos los mensajes del subsistema ETH (“todos” incluye cualquier mensaje codificado para “error,” “información” o “rastreo”) se anotarán cronológicamente de forma remota basándose en los valores de log_user y log_info del sistema principal remoto.

Utilice los mandatos **list all** o **list status** para visualizar lo que ha establecido con los mandatos **noremove** y **remote**.

Set

Utilice el mandato **set** para establecer el número máximo de identificadores por segundo, la característica de la indicación de la hora o para establecer las opciones de rastreo.

Sintaxis:

```
set pin . . .  
remote-logging . . .  
timestamp . . .  
trace . . .
```

pin *detecciones_máx*

Utilice el mandato **set pin** para establecer el parámetro pin en el número máximo de detecciones que pueden enviarse por segundo. Internamente, pin se restablece cada décima de segundo. (Una décima parte del número (*detecciones_máx*) se envía cada décima de segundo.)

remote-logging

Utilice el mandato **set remote-logging** para configurar las opciones de anotación cronológica remota. Cuando estas opciones se configuran desde el entorno de supervisión, los cambios surten efecto inmediatamente y vuelven a sus valores configurados previamente cuando se reanuda el dispositivo.

Sintaxis:

```
set remote-logging on  
off
```

Mandatos de configuración ELS (Talk 6)

`facility . . .`
`level . . .`
`no-msgs`
`remote_ip_addr . . .`
`source_ip_addr ...`
`local_id`

- on** Activa la anotación cronológica remota. Ahora la anotación cronológica remota está habilitada para permitir que cualquier mensaje seleccionado por el mandato **remote** se anote cronológicamente de manera activa.
- off** Desactiva la anotación cronológica remota. Se impedirá que todos los mensajes seleccionados por el mandato 'remote' se anoten cronológicamente.

facility

Especifica un valor que, en combinación con el valor de *nivel*, se utiliza por el daemon de la anotación cronológica del sistema en la estación de trabajo remota para determinar dónde se anotan cronológicamente los mensajes. Este valor se utiliza para todos los mensajes ELS anotados cronológicamente de forma remota a menos que especifique un valor diferente para un suceso ELS, rango, grupo o subsistema en particular con el mandato **remote**.

Estos son todos los posibles valores de recurso de anotaciones cronológicas del sistema:

- log_auth
- log_authpriv
- log_cron
- log_daemon
- log_kern
- log_lpr
- log_mail
- log_news
- log_syslog
- log_user
- log_uucp
- log_local0-7

- level** Especifica un valor que, junto con el valor de *recurso*, utiliza el daemon de la anotación cronológica del sistema en la estación de trabajo remota para determinar dónde se han de anotar los mensajes. Este valor se utiliza para todos los mensajes ELS anotados cronológicamente de forma remota a menos que especifique un valor diferente para un suceso ELS, rango, grupo o subsistema en particular con el mandato **remote**.

Estos son todos los valores posibles de nivel de anotación cronológica del sistema:

- log_emerg
- log_alert
- log_crit
- log_err
- log_warning

Mandatos de configuración ELS (Talk 6)

log_notice
log_info
log_debug

no-msgs

Especifica el número de mensajes en el almacenamiento intermedio para la anotación cronológica remota antes de que ésta se reinicie.

remote_ip_addr

Se trata de una dirección ip con el formato xxx.xxx.xxx.xxx donde xxx puede ser cualquier entero de 0 a 255. Representa la dirección ip del sistema principal remoto donde residen los archivos de anotación cronológica.

source_ip_addr

Se trata de una dirección ip con el formato xxx.xxx.xxx.xxx donde xxx puede ser cualquier entero de 0 a 255.

Debe utilizar una dirección IP que esté configurada en el 2216 para una identificación más fácil cuando aparece la dirección IP o el nombre de sistema principal en el mensaje ELS anotado cronológicamente de forma remota. También debe verificar que el servidor de nombres resuelva rápidamente esta dirección IP en un nombre de sistema principal o que al menos el servidor de nombres responda rápidamente con un mensaje de “dirección no encontrada.”

Para determinar que la dirección IP se resuelve correctamente entre el mandato **host** en la estación de trabajo tal como se muestra:

```
workstation>host 5.1.1.1  
host: address 5.1.1.1 NOT FOUND  
workstation>
```

Si la respuesta tarda más de 1 segundo, seleccione una dirección IP que se resuelva más rápidamente.

local_id

Se trata de cualquier serie de 32 caracteres como máximo, que se incluye en el mensaje anotado cronológicamente en el archivo remoto y puede ayudarle a identificar qué máquina ha anotado cronológicamente el mensaje.

timestamp [timeofday o uptime u off]

Le permite activar la indicación de la hora en el mensaje para que aparezca la hora del día o el tiempo de activación (horas, minutos y segundos, sin fecha, desde que se ha inicializado por última vez el dispositivo) junto a cada mensaje. También se puede desactivar la indicación de la hora.

Utilice el mandato **set timestamp** para habilitar una de las opciones de indicación de la hora siguientes.

timeofday

Añade el prefijo HH:MM:SS a cada mensaje ELS indicando la hora de aparición con el formato de 24 horas.

uptime

Añade el prefijo HH:MM:SS a cada mensaje ELS indicando la hora de la aparición durante un ciclo de 100 horas. Después de 100

Mandatos de configuración ELS (Talk 6)

horas de tiempo de activación, el contador de tiempo de activación vuelve a cero para empezar otro ciclo de 100 horas.

off Desactiva el prefijo de indicación de la hora ELS.

trace Utilice el mandato **set trace** para configurar las opciones de rastreo. Si configura las opciones de rastreo desde el entorno de supervisión, los cambios surten efecto inmediatamente. Vuelven a los valores configurados previamente cuando se reanuda el dispositivo.

Nota: El rastreo sólo debe utilizarse bajo indicación del personal de soporte especializado. El rastreo, especialmente cuando se utiliza con la copia continua en disco activada, utiliza recursos de dispositivo y puede influir en el rendimiento y productividad globales.

Sintaxis:

set trace *decode*
default-bytes-per-pkt
disk-shadowing
max-bytes-per-pkt
memory-trace-buffer-size
off
on
reset
stop-event
wrap-mode

decode *off/on*

Activa y desactiva la decodificación de paquetes. No todos los componentes soportan la decodificación de paquetes.

default-bytes-per-pkt *bytes*

Establece el número por omisión de bytes rastreados. Este valor se utiliza si el componente que efectúa el rastreo no especifica ningún valor.

disk-shadowing **[[off u on] o record-size o time-limit o delete-file o max-file-size]**

Activa y desactiva la copia continua en disco, establece el tamaño máximo de archivo de rastreo o establece el tiempo máximo para los rastreos con copia continua en disco.

[off u on]

Activa o desactiva la copia continua en disco. Si la copia continua en disco está habilitada, los registros de rastreo se copian en el disco duro. Una vez copiado un registro de rastreo en el disco duro, ya no se puede visualizar desde la supervisión.

Nota: La copia continua en disco debe establecerse en OFF siempre que se emitan los mandatos de software WRITE, TFTP software, RETRIEVE de vuelco del sistema o COPY.

disk-shadowing delete-file

Suprime el archivo de rastreo.

disk-shadowing max-file-size *Mbytes*

Establece el tamaño máximo de archivo para el archivo de rastreo.

Mandatos de configuración ELS (Talk 6)

Valores válidos: De 1 MB a 16 MB

Valor por omisión: 10

disk-shadowing record-size *bytes*

Establece el tamaño de registro para los registros del archivo de rastreo:

Valores válidos

1024, 2048 ó 4096 bytes

Valor por omisión

2048 bytes

Notas:

1. Si ya existe un archivo de rastreo, se visualiza "Cannot change Record Size without first deleting the existing Trace File" y no se cambia el tamaño de registro.
2. Si configura un tamaño de registro y ya existe un archivo de rastreo, el rastreo utilizará el tamaño de registro del archivo existente.

disk-shadowing time-limit *horas*

Establece el tiempo máximo para la copia continua en disco de los rastreos:

Valores válidos

De 1 a 72 horas

Valor por omisión

24 horas

Nota: Se detiene la copia continua en disco (el rastreo continúa) después de que transcurra este tiempo. El tiempo real se restablece en 0 cuando se vuelve a activar la copia continua en disco.

max-bytes-per-pkt *bytes*

Establece el número máximo de bytes rastreados para cada paquete.

memory-trace-buffer-size *bytes*

Establece el tamaño, en bytes, del almacenamiento intermedio de rastreo de RAM.

Valores válidos: 0, ≥ 10.000

Valor por omisión: 0

off Inhabilita el rastreo de paquetes.

on Habilita el rastreo de paquetes.

reset Borra el almacenamiento intermedio de rastreo y restablece todos los contadores asociados.

stop-event *id suceso*

Detiene el rastreo cuando se produce un suceso (id suceso). Entre un id de suceso ELS (por ejemplo: TCP.013) o "Ninguno". "Ninguno" es el valor por omisión. El rastreo sólo se detiene si está habilitada la visualización del suceso ELS en particular.

Mandatos de configuración ELS (Talk 6)

Cuando se produce un suceso de detención, se graba una entrada en el almacenamiento intermedio de rastreo. El mandato **view** para esta entrada de rastreo visualizará "Tracing stopped due to ELS Event Id: TCP.013".

Después de que se detenga el rastreo debido a un suceso de detención, debe volver a habilitar el rastreo con el mandato **set trace on**. (Un reinicio también volverá a habilitar el rastreo si se ha habilitado desde el indicador ELS Config>.)

wrap-mode [off u on]

Activa y desactiva la modalidad de reinicio del almacenamiento intermedio de rastreo. Si la modalidad de reinicio está activada y el almacenamiento intermedio de rastreo está lleno, se grabará encima de los registros de rastreo anteriores con los nuevos registros de rastreo cuando sea necesario para continuar el rastreo.

Trace

Habilita el rastreo de paquetes para el suceso/rango/subsistema/grupo especificado. Cuando se utiliza el mandato **trace** desde el indicador ELS Config>, los cambios pasan a formar parte de la configuración y es necesario rearmar para activar los cambios.

Sintaxis:

```
trace                event . . .  
                    group . . .  
                    range . . .  
                    subsystem . . .
```

event *subsistema.númerosuceso*

Hace que se visualice el suceso de rastreo especificado (*subsistema.númerosuceso*) en la supervisión del sistema.

group *nombregrupo*

Permite visualizar los sucesos de rastreo que se han añadido previamente al grupo especificado, en el dispositivo que supervisa.

range *nombresubsistema número_primer_suceso número_último_suceso*

Donde *número_primer_suceso* es el número del primer suceso del rango de sucesos especificado y *número_último_suceso* es el número del último suceso del rango de sucesos especificado.

Hace que se visualicen los sucesos de rastreo del rango especificado para el subsistema especificado, en la supervisión del sistema.

Ejemplo:

```
trace range gw 19 22
```

Hace que se visualicen los sucesos de rastreo gw.19, gw.20, gw.21 y gw.22 en la supervisión del sistema.

subsystem *nombresubsistema*

Permite visualizar los sucesos de rastreo asociados con el subsistema especificado en el dispositivo que supervisa.

Trap

Utilice el mandato **trap** para seleccionar el mensaje que se ha de enviar a la estación de trabajo de gestión de la red SNMP remota. Una estación de trabajo de gestión de la red SNMP remota es un sistema principal IP que actúa como un gestor SNMP.

Sintaxis:

```
trap                event . . .
                    group . . .
                    range . . .
                    subsystem . . .
```

event *subsistema.númerosuceso*

Hace que el mensaje especificado (*subsistema.númerosuceso*) se envíe a la estación de trabajo de gestión de la red en una detección SNMP.

group *nombregrupo*

Permite enviar los mensajes, que se han añadido previamente al grupo especificado, a una estación de trabajo de gestión de la red en una detección SNMP.

range *nombresubsistema número_primer_suceso número_último_suceso*

Donde *número_primer_suceso* es el número del primer suceso del rango de sucesos especificado y *número_último_suceso* es el número del último suceso del rango de sucesos especificado.

Hace que se envíen los mensajes, que están en el rango especificado para el subsistema especificado, a una estación de trabajo de gestión de la red en una detección SNMP.

Ejemplo:

```
trap range gw 19 22
```

Hace que se envíen los mensajes de los sucesos gw.19, gw.20, gw.21 y gw.22 a una estación de trabajo de gestión de la red en una detección SNMP.

subsystem *nombresubsistema*

Permite que se envíen los mensajes asociados con el subsistema especificado a una estación de gestión en una detección SNMP.

Nota: Los mensajes para los subsistemas IP ICMP, ARP y UDP no pueden enviarse en detecciones SNMP porque estas áreas se utilizan, o pueden utilizarse, en el proceso de envío de la detección SNMP. Esto podría conducir a un bucle infinito de tráfico haciendo que el dispositivo tuviese que realizar un esfuerzo indebido.

Mandatos de configuración de filtros de red ELS

Los filtros de red ELS le proporcionan la posibilidad de consultar únicamente los mensajes ELS con determinados números de red y descartando el resto de mensajes ELS.

Cuando se crea un filtro, se especifica el subsistema, suceso o rango de sucesos a los que se aplica el filtro. También puede especificar la cola (por ejemplo,

Mandatos de configuración ELS (Talk 6)

“DISPLAY”, “TRAP”, “TRACE” o “REMOTE-LOGGING”). Finalmente, se especifica el número de red (o rango de números de red) que desea filtrar.

Cuando habilita el filtro, los mensajes que se han activado mediante mandatos ELS se someten al filtro. El filtro sólo permite mensajes con los números de red especificados. El filtro hace que el dispositivo descarte los mensajes que no contienen los números de red especificados.

Mediante la reducción del número de mensajes ELS enviados, puede localizar con más facilidad los mensajes para las interfaces en las que está interesado.

Esta sección describe los mandatos para configurar los filtros de red ELS. Para configurar estos filtros, entre el mandato **filter net** en el indicador ELS>. Después, entre los mandatos de configuración en el indicador ELS Filter net>.

Tabla 16. Mandatos de configuración de filtros de red ELS

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página 10.
Create	Crea un filtro y le asigna un número. Están permitidos un máximo de 64 filtros.
Delete	Suprime un número de filtro especificado o todos los filtros.
Disable	Inhabilita un número de filtro especificado o todos los filtros.
Enable	Habilita un número de filtro especificado o todos los filtros.
List	Lista un número de filtro especificado o todos los filtros.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página 11.

Create

Utilice el mandato **create** para crear un filtro de red ELS.

Sintaxis:

```
create queue event nombre_suceso númerored_inicio  
númerored_final  
  
range rango_sucesos númerored_inicio  
númerored_final  
  
subsystem nombre_subsistema númerored_inicio  
númerored_final
```

queue La cola para la que establece el filtro. Las colas válidas son:

- Visualización
- Rastreo
- Detección
- Remota

event *nombre_suceso númerored_inicio númerored_final*

Especifica el suceso y los números de red que está filtrando.

Si especifica el mismo número para *inicio_red#* y *final_red#*, está filtrando un solo número de red.

El mandato **create trap event GW.009 2 10** filtra las detecciones para el mensaje GW.009 para los números de red del 2 al 10.

Mandatos de configuración ELS (Talk 6)

range *rango_sucesos número_inicio número_final*

Especifica el rango de mensajes ELS y números de red que está filtrando.

Si especifica el mismo número para *inicio_red#* y *final_red#*, está filtrando un solo número de red.

El mandato **create remote range ipx 19 22 3 6** filtra todos los mensajes ipx empezando por IPX.019 y finalizando en IPX.022 para los números de red del 3 al 6 para la anotación cronológica remota.

subsystem *nombre_subsistema número_inicio número_final*

Especifica el subsistema y los números de red que está filtrando.

Si especifica el mismo número para *inicio_red#* y *final_red#*, está filtrando un solo número de red.

El mandato **create display subsys ip 1 1**, filtra todos los mensajes ELS para el subsistema ip que contiene el número de red 1 para su visualización. Se descartan todos los demás mensajes del subsistema ip.

Delete

Utilice el mandato **delete** para suprimir un filtro ELS específico o todos los filtros ELS.

Sintaxis:

```
delete                all
                        filter númerofiltro
```

all Suprime todos los filtros configurados actualmente.

filter *númerofiltro*

Suprime el filtro especificado por *númerofiltro*. Utilice el mandato **list** para obtener el número del filtro que desea suprimir.

Disable

Utilice el mandato **disable** para inhabilitar un filtro ELS específico o todos los filtros ELS.

Sintaxis:

```
disable              all
                        filter númerofiltro
```

all Inhabilita todos los filtros configurados actualmente.

filter *númerofiltro*

Inhabilita el filtro especificado por *númerofiltro*. Utilice el mandato **list** para obtener el número del filtro que desea inhabilitar.

Enable

Utilice el mandato **enable** para habilitar un filtro ELS específico o todos los filtros ELS.

Sintaxis:

```
enable               all
                        filter númerofiltro
```

all Habilita todos los filtros configurados actualmente.

Mandatos de configuración ELS (Talk 6)

filter *númerofiltro*

Habilita el filtro especificado por *númerofiltro*. Utilice el mandato **list** para obtener el número del filtro que desea habilitar.

List

Utilice el mandato **list** para listar un filtro ELS específico o todos los filtros ELS.

Sintaxis:

```
list                all
                    filter númerofiltro
```

all Lista todos los filtros configurados actualmente.

filter Lista el filtro especificado por *númerofiltro*.

Mandatos de configuración de almacenamiento intermedio de mensajes ELS

La Tabla 17 describe los mandatos disponibles en el indicador ELS Config Advanced>.

Tabla 17. Mandatos de configuración de almacenamiento intermedio de mensajes ELS

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página 10.
List	Visualiza los valores de configuración para el almacenamiento intermedio de mensajes.
Log	Habilita la anotación cronológica de los mensajes seleccionados en el almacenamiento intermedio de mensajes.
Nolog	Desactiva la anotación cronológica de los mensajes seleccionados en el almacenamiento intermedio de mensajes.
Set	Establece el tamaño del almacenamiento intermedio de mensajes, la modalidad de reinicio, si se produce o no la anotación cronológica, qué suceso finalizará el almacenamiento intermedio de mensajes y lo que hace el sistema cuando se detiene el almacenamiento intermedio por un suceso.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página 11.

List

Utilice el mandato **list** para listar la configuración del almacenamiento intermedio de mensajes ELS.

Sintaxis:

```
list                status
```

Ejemplo:

```
ELS Config Advanced> list status
-----Configuration-----
Logging Status:  OFF   Wrap Mode:  ON   Logging Buffer Size:  8500   Kbytes
Stop-Event:    APPN.2   Stop-String:  netdn for intf 6
Additional Stop-Action:  NONE
```

Consulte la sección “Set” en la página 178 para ver la descripción de los mandatos que cambian los valores de la pantalla.

Log

Utilice el mandato **log** para seleccionar los mensajes que se anotarán cronológicamente en el almacenamiento intermedio de mensajes.

Sintaxis:

```
log                event  
                   group  
                   range  
                   subsystem
```

event *subsistema.númerosuceso*

Hace que se anote cronológicamente el mensaje especificado (*subsistema.númerosuceso*) en el almacenamiento intermedio de mensajes.

group *nombregrupo*

Permite que los mensajes que se habían añadido previamente al grupo especificado se anoten cronológicamente en el almacenamiento intermedio de mensajes.

range *nombresubsistema número_primer_suceso número_último_suceso*

Donde *número_primer_suceso* es el número del primer suceso del rango de sucesos especificado y *número_último_suceso* es el número de último suceso del rango de sucesos especificado.

Hace que los mensajes del rango especificado para el subsistema especificado se anoten cronológicamente en el almacenamiento intermedio de mensajes.

Ejemplo:

```
log range gw 19 22
```

Hace que se anoten cronológicamente los mensajes de los sucesos gw.19, gw.20, gw.21 y gw.22 en el almacenamiento intermedio de mensajes.

subsystem *nombresubsistema*

Permite que los mensajes asociados con el subsistema especificado se anoten cronológicamente en el almacenamiento intermedio de mensajes.

Nolog

Utilice el mandato **nolog** para eliminar los mensajes de la lista de mensajes definida que se anotan cronológicamente en el almacenamiento intermedio de mensajes.

Sintaxis:

```
nolog             event  
                  group  
                  range  
                  subsystem
```

event *subsistema.númerosuceso*

Hace que no se anote cronológicamente el mensaje especificado (*subsistema.númerosuceso*) en el almacenamiento intermedio de mensajes.

Mandatos de configuración ELS (Talk 6)

group *nombregrupo*

Permite que los mensajes que se habían añadido previamente al grupo especificado no se anoten cronológicamente en el almacenamiento intermedio de mensajes.

range *nombresubsistema número_primer_suceso número_último_suceso*

Donde *número_primer_suceso* es el número del primer suceso del rango de sucesos especificado y *número_último_suceso* es el número del último suceso del rango de sucesos especificado.

Hace que los mensajes que están en el rango especificado para el subsistema especificado no se anoten cronológicamente en el almacenamiento intermedio de mensajes.

Ejemplo:

```
log range gw 19 22
```

Hace que no se anoten cronológicamente los mensajes de los sucesos gw.19, gw.20, gw.21 y gw.22 en el almacenamiento intermedio de mensajes.

subsystem *nombresubsistema*

Permite que los mensajes asociados con el subsistema especificado no se anoten cronológicamente en el almacenamiento intermedio de mensajes.

Set

Utilice el mandato **set** para configurar distintas opciones del almacenamiento intermedio de mensajes ELS.

Sintaxis:

```
set                buffer-size Kbytes  
                   logging [on u off]  
                   stop action . . .  
                   stop event subsistema.númerosuceso  
                   stop string texto  
                   wrap on u off]
```

buffer-size *Kbytes*

Especifica el tamaño, en kilobytes, del almacenamiento intermedio de mensajes que el sistema debe asignar. El mandato **mem** visualiza esta memoria como Never Alloc. Si se establece este valor demasiado alto podría impedir que el dispositivo funcionase correctamente después del arranque debido a que no hay suficiente memoria para los protocolos y características.

Valores válidos: De 0 KB al 60% de la memoria disponible en el dispositivo.

Valor por omisión: 0 (sin almacenamiento intermedio de mensajes)

Nota: Debe asignar un almacenamiento intermedio con este mandato antes de poder activar la anotación cronológica.

logging *[on u off]*

Especifica si se producirá el almacenamiento intermedio de mensajes. Este mandato no surtirá efecto hasta que asigne un almacenamiento intermedio utilizando el mandato **set buffer-size**. El valor por omisión es desactivado.

Mandatos de configuración ELS (Talk 6)

stop action [appn-dump o disk-offload o none o system-dump]

Especifica la acción adicional que el sistema efectúa cuando se produce el “suceso de detención” (y si se especifica, la “serie de detención”). Las acciones son:

appn-dump

Vuelca el protocolo APPN, si está activo. El vuelco APPN indicará que el vuelco se ha realizado como resultado de una acción de detención.

disk-offload

Graba una versión formateada del almacenamiento intermedio en un archivo de la unidad de disco duro. Si ya existe el archivo, el nuevo archivo lo sustituye. Después, puede utilizar el mandato de supervisión **tftp file** para enviar el archivo a un sistema principal remoto.

none No se efectúa ninguna otra acción después de detenerse la anotación cronológica.

system-dump

Vuelca todo el sistema. El vuelco del sistema indicará que se ha realizado el vuelco como resultado de una acción de detención.

Valor por omisión: ninguno

stop event [subsistema.númerosuceso o none]

Especifica el suceso (*subsistema.númerosuceso*) que detiene la anotación cronológica. Si ha especificado una serie de detención, el texto de la serie de detención también debe coincidir. Cuando se produce el suceso de detención:

1. Si NO se ha especificado ninguna acción de detención (el valor *ninguno*), se anotan cronológicamente los cinco mensajes ELS siguientes. Sin embargo, si se ha especificado una acción de detención (un valor distinto de *ninguno*), no se anotan cronológicamente más mensajes ELS.
2. Se detiene la anotación cronológica.
3. El sistema realiza la “acción de detención” especificada.

La anotación cronológica permanece detenida hasta la próxima vez que se emite el mandato **set logging on** o que se reanuda el dispositivo.

Si no especifica el suceso de detención cuando entra el mandato, el sistema le solicita que entre el suceso de detención. La especificación de **none** inhabilita la función del suceso de detención.

Valor por omisión: ninguno

stop string *texto* o none

Especifica la serie que se ha de utilizar conjuntamente con el “suceso de detención” para detener la anotación cronológica. Si no ha especificado ningún suceso de detención, el sistema pasa por alto la “serie de detención.”

El *texto* puede ser cualquier serie ASCII de hasta 32 caracteres de longitud. Si no especifica el *texto* cuando entra el mandato, el sistema le solicitará la serie. Si se entra **none** se borra la “serie de detención.”

Valor por omisión: none

Mandatos de configuración ELS (Talk 6)

wrap [on u off]

Especifica si se ha de detener la anotación cronológica cuando el almacenamiento intermedio esté lleno (off) o si se han de anotar los nuevos mensajes al principio del almacenamiento intermedio (on).

Valor por omisión: on

Entrada y salida del entorno operativo ELS

El entorno de supervisión ELS (disponible desde el proceso GWCON) se caracteriza por el indicador ELS>. Los mandatos entrados en este indicador modifican los valores actuales de parámetros ELS. Estos mandatos se describen en la sección “Capítulo 11. Configuración y supervisión del Sistema de anotación cronológica de sucesos (ELS)” en la página 157.

Para entrar en el entorno de supervisión ELS desde OPCON:

1. Entre el mandato **console**.

* console

La supervisión visualiza el indicador GWCON (+). Si el indicador no aparece cuando entra por primera vez en GWCON, pulse **Intro**.

2. En el indicador GWCON, entre el mandato siguiente para acceder a ELS:

+ event

La supervisión visualiza el indicador de supervisión ELS (ELS>). Ahora, puede entrar los mandatos de supervisión ELS.

Para salir del entorno de supervisión ELS, entre el mandato **exit**.

Mandatos de supervisión ELS

Esta sección resume y después explica todos los mandatos de supervisión ELS. Después de acceder al entorno de supervisión ELS, puede entrar mandatos de supervisión ELS en el indicador ELS>.

Tabla 18. Resumen de los mandatos de supervisión ELS

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página 10.
Advanced	Le lleva al entorno de configuración avanzada, en el que puede configurar el almacenamiento intermedio de mensajes.
Clear	Restablece a cero las cuentas de mensajes asociadas con los sucesos, grupos o subsistemas especificados.
Display	Habilita la visualización de mensajes en la consola.
Exit	Sale del proceso de consola ELS y devuelve el usuario a GWCON.
Filter	Filtra los mensajes ELS basándose en el número de red.
List	Lista la información sobre los valores y mensajes ELS.
Nodisplay	Inhabilita la visualización de mensajes en la consola.
Noremote	Inhabilita la anotación cronológica remota en el archivo de la estación de trabajo remota.
Notrace	Inhabilita la visualización de sucesos de rastreo en la consola.
Notrap	Impide que los mensajes se envíen en detecciones SNMP a la estación de trabajo de gestión de la red.

Mandatos de supervisión ELS (Talk 5)

Tabla 18. Resumen de los mandatos de supervisión ELS (continuación)

Mandato	Función
Packet-trace	Proporciona un entorno central ampliado para establecer y listar los parámetros de rastreo de paquetes activos.
Remote	Permite que los mensajes se anoten cronológicamente en un archivo de una estación de trabajo remota.
Remove	Libera memoria borrando la información almacenada.
Restore	Borra los valores actuales y vuelve a cargar la configuración ELS inicial.
Retrieve	Vuelve a cargar la configuración ELS guardada.
Save	Almacena la configuración actual.
Set	Establece el parámetro pin y la característica de indicación de la hora.
Statistics	Visualiza los subsistemas disponibles y las estadísticas pertinentes.
Trace	Habilita la visualización de sucesos de rastreo en la consola.
Trap	Permite enviar los mensajes a una estación de trabajo de gestión de la red en detecciones SNMP.
View	Permite la visualización de los paquetes rastreados.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página 11.

Advanced

Utilice el mandato **advanced** para entrar en el entorno de supervisión avanzada. En este entorno se cambia el funcionamiento del almacenamiento intermedio de mensajes.

Sintaxis:

advanced

Clear

Utilice el mandato **clear** para restablecer a cero las cuentas de los mandatos de visualización, rastreo, detección o remoto que sean relativos a sucesos, grupos o subsistemas específicos.

Sintaxis:

```
clear          event . . .
                group . . .
                subsystem . . .
```

event *subsistema. númerosuceso*

Restablece la cuenta de sucesos a cero para la visualización, la detección, el rastreo o la anotación cronológica remota del suceso especificado (*subsistema.número-suceso*).

group *nombre.grupo*

Restablece la cuenta de sucesos a cero para la visualización, detección, rastreo o anotación cronológica remota del grupo especificado (*nombre.grupo*).

subsystem *nombre.subsistema*

Restablece la cuenta de sucesos a cero para la visualización, detección, rastreo o anotación cronológica remota del subsistema especificado (*nombre.subsistema*).

Mandatos de supervisión ELS (Talk 5)

Display

Utilice el mandato `display` para habilitar la visualización de mensajes en el monitor de supervisión para sucesos específicos.

Sintaxis:

```
display          event . . .  
                  group . . .  
                  range . . .  
                  subsystem . . .
```

event *subsistema.númerosuceso*

Visualiza mensajes para el suceso especificado (subsistema.númerosuceso).

group *nombregrupo*

Visualiza los mensajes para un grupo especificado (*nombregrupo*).

range *nombresubsistema número_primer_suceso número_último_suceso*

Donde *número_primer_suceso* es el número del primer suceso del rango de sucesos especificado y *número_último_suceso* es el número del último suceso del rango de sucesos especificado.

Visualiza un rango de mensajes para el subsistema especificado.

Ejemplo:

```
display range gw 19 22
```

Visualiza los sucesos gw.19, gw.20, gw.21 y gw.22.

subsystem *nombre.subsistema*

Visualiza cualquier mensaje asociado con el subsistema especificado (*nivel de anotación cronológica*). Si no especifica ningún nivel de anotación cronológica, se activan todos los mensajes para ese subsistema.

Files Trace TFTP

Utilice el mandato **files trace tftp** para recuperar archivos de rastreo del subdirectorio asociado con:

- El banco activo actualmente (banco A o Banco B del disco duro)
- El Banco A del disco duro
- El Banco B del disco duro
- El archivo de rastreo almacenado en el Subdirectorio de red (si no hay ningún banco activo)

Sintaxis:

```
files trace tftp  active-bank ...  
                  bank-a ...  
                  bank-b ...  
                  net-subdir ...
```

Se le solicita la *dirección IP del servidor remoto* y la *vía de acceso remota/nombre de archivo*.

active-bank

Recupera el archivo de rastreo del banco activo actualmente

bank-a

Recupera el archivo de rastreo del banco A

bank-b

Recupera el archivo de rastreo del banco B

net-subdir

Recupera el archivo de rastreo almacenado en el Subdirectorío de red (si no hay ningún banco activo)

Filter

Utilice el mandato **filter** para acceder al entorno de mandatos de configuración de filtros. Consulte la sección “Mandatos de la supervisión de filtros de red ELS” en la página 204 para ver los detalles completos de los mandatos.

Sintaxis:

filter net

List

Utilice el mandato **list** para obtener información actualizada relativa a los valores ELS y para obtener listados de los mensajes seleccionados.

Sintaxis:

list active . . .
all
event . . .
filter-status
groups . . .
pin
remote-log status
subsystem . . .
trace-status

all Lista todos los subsistemas, grupos definidos, subsistemas habilitados, sucesos habilitados y pin.

active *nombre.subsistema*

Visualiza los sucesos que están activos para un subsistema específico o que tienen cuentas de mensajes que no son cero.

Ejemplo:

```
list active ip
Event      Active  Count  Message
IP.007          2874  %I -> %I
IP.022           13  add nt %I int %I nt %n int %s/%d
IP.036          2874  rcv pkt prt %d frm %I
IP.058           23  del nt %I rt via %I nt %n int %s/%d
IP.068           37  routing cache cleared
D=Display on  T=Trap on  P=Packet Trace on  F=Filter on  R=Remote Logging on
A=Advanced on
```

Si la Anotación cronológica remota está activada, los sucesos visualizados como activos para un subsistema tienen una “R” junto a su nombre.

Mandatos de supervisión ELS (Talk 5)

event *subsistema.númersuceso*

Visualiza el nivel de anotación cronológica, el mensaje y la cuenta del suceso especificado.

Ejemplo:

```
list event ip.007
```

```
Level: p-TRACE  
Message: source_ip_address -> destination_ip_address  
Active: Count: 84182
```

Si se ha activado la Anotación cronológica remota para este suceso y los valores de *recurso_anotación_cronológica_sistema* y *nivel_anotación_cronológica_sistema* eran *log_daemon* y *log_crit*, las últimas líneas serían:

```
Active: R count:84182  
Syslog Facility: log_daemon Syslog Level: log_crit
```

filter-status

Lista los filtros de números de red ELS.

groups *nombre.grupo*

Visualiza los nombres de grupos definidos por el usuario.

pin Lista el número actual de mensajes de sucesos ELS enviados por segundo en detecciones SNMP. Es un valor de umbral que puede utilizarse para reducir la cantidad de tráfico de detección SNMP.

Ejemplo:

```
list pin
```

```
Pin: 100 events/second
```

remote-log status

Lista los valores actuales de las opciones de anotación cronológica remota en el mandato **set remote-logging**.

Ejemplo:

```
list r
```

```
Remote Logging is On  
Source Ip Address = 192.9.200.8  
Remote Log IP Address = 192.9.200.1  
Default Syslog Facility = LOG_USER  
Default Syslog Priority Level = LOG_INFO  
Number of Messages in Remote Log = 256  
Remote Logging Local ID = SPHINX
```

subsystem *nombre.subsistema*

Lista los nombres de suceso, el número total de sucesos que se han producido y sus descripciones.

Nota: Aunque ELS soporta todos los subsistemas del dispositivo, no todos los dispositivos soportan todos los subsistemas. Consulte *ELS Messages* para ver una lista de subsistemas soportados actualmente.

subsystem *nombre.subsistema*

Lista todos los sucesos, niveles de anotación cronológica y mensajes para el subsistema especificado.

Ejemplo:

```
list subsystem eth
```

```
Event      Level      Message  
ETH.001    P-TRACE    brd rcv unkwn type packet_type source_Ethernet_address ->  
destination_Ethernet_address nt network  
ETH.002    UE-ERROR    rcv unkwn typ packet_type source_Ethernet_address ->
```

Mandatos de supervisión ELS (Talk 5)

```
ETH.010 C-INFO destination_Ethernet_address nt network
LLC unk SAP DSAP source_Ethernet_address ->
destination_Ethernet_address nt network
```

subsystem all

Lista todos los sucesos, niveles de anotación cronológica y mensajes para cada suceso que se ha producido en el dispositivo.

trace-status

Visualiza información sobre el estado del rastreo de paquetes, incluyendo la información de configuración y de tiempo de ejecución.

Ejemplo:

```
list trace-status
```

```
----- Configuration -----
Trace Status:ON Wrap Mode:ON Decode Packets:ON HD Shadowing:ON
RAM Trace Buffer Size:100000 Maximum Trace Buffer File Size:10000000
Max Packet Bytes Trace:256 Default Packet Bytes Traced:100
Trace File Record Size:2048 Stop Trace Event: TCP.013
Maximum Hours to HD Shadow: 1
----- Run-time Status -----
Packets in RAM Trace Buffer:1 Free Trace Buffer Memory:99958
Trace Errors:0 First Packet:1 Last Packet:1
Trace Records Stored on HD:8 Trace Buffer File Size:16560
HD-Shadowing Time Exceeded? NO Elapsed Time: 0 hr, 0 min, 10 sec
Has Stop Trace Event Occurred? NO
```

- “Trace Status” de la pantalla LIST TRACE-STATUS indicará OFF cuando se produzca una acción STOP-ON-EVENT.
- “HD Shadowing” de la pantalla LIST TRACE-STATUS indicará OFF cuando se produzca la acción STOP-ON-EVENT o cuando se exceda el Límite de tiempo.
- “Trace Buffer File Size” mostrará <wrapped> cuando se haya producido un reinicio en el archivo de rastreo.
- Si se excede el límite de tiempo de copia continua en disco, pero no se ha grabado ningún registro de rastreo desde que el tiempo ha caducado, se visualizará “HD-Shadowing Time Exceeded? NO < Next trace will turn it OFF>”. Cuando se haya grabado el siguiente registro de rastreo, se visualizará “HD-Shadowing Time Exceeded? YES”.

El mandato ELS Config>**LIST TRACE** bajo **talk 6** visualiza información similar a la siguiente:

```
----- Configuration -----
Trace Status:ON Wrap Mode:ON Decode Packets:ON HD Shadowing:ON
RAM Trace Buffer Size:100000 Maximum Trace Buffer File Size:10000000
Max Packet Bytes Trace:256 Default Packet Bytes Traced:100
Trace File Record Size:2048 Stop Trace Event: TCP.013
Maximum Hours to HD Shadow: 1
```

Nodisplay

Utilice el mandato **nodisplay** para seleccionar y desactivar la visualización de mensajes en la consola.

Sintaxis:

```
nodisplay          event . . .
                    group . . .
                    range . . .
                    subsystem . . .
```

event *subsistema.numerosuceso*

Suprime la visualización de mensajes para el suceso especificado.

Mandatos de supervisión ELS (Talk 5)

group *nombre.grupo*

Suprime la visualización de mensajes que se han añadido previamente al grupo especificado (*nombre.grupo*).

range *nombresubsistema número_primer_suceso número_último_suceso*

Donde *número_primer_suceso* es el número del primer suceso del rango de sucesos especificado y *número_último_suceso* es el número del último suceso del rango de sucesos especificado.

Suprime la visualización de un rango de mensajes para el subsistema especificado.

Ejemplo:

```
nodisplay range gw 19 22
```

Suprime la visualización de los sucesos gw.19, gw.20, gw.21 y gw.22.

subsystem *nombre.subsistema*

Suprime la visualización de los mensajes asociados con el subsistema especificado (*nivel de anotación cronológica*).

Noremote

Utilice el mandato **noremote** para seleccionar y desactivar la anotación cronológica de mensajes en una estación de trabajo remota.

Sintaxis:

```
noremote                event . . .  
                        group . . .  
                        range . . .  
                        subsystem . . .
```

event *subsistema.númerosuceso*

Suprime la anotación cronológica remota de mensajes para el suceso especificado.

group *nombre.grupo*

Suprime la anotación cronológica remota de mensajes que se han añadido previamente al grupo especificado (*nombre.grupo*).

range *nombresubsistema número_primer_suceso número_último_suceso*

Donde *número_primer_suceso* es el número del primer suceso del rango de sucesos especificado y *número_último_suceso* es el número del último suceso del rango de sucesos especificado.

Suprime la anotación cronológica remota de un rango de mensajes para el subsistema especificado.

Ejemplo:

```
noremote range gw 19 22
```

Suprime la anotación cronológica remota de los sucesos gw.19, gw.20, gw.21 y gw.22

subsystem *nombre.subsistema*

Suprime la anotación cronológica remota de los mensajes asociados con el subsistema especificado (*nivel de anotación cronológica*).

Ejemplo:

```
noremote subsystem tkr
```

Nota: Con `noremote`, no hay necesidad de especificar el Recurso y Nivel de anotación cronológica del sistema, a diferencia de `Remote`.

Utilice los mandatos **list event** y **list active** para verificar lo que ha establecido con los mandatos **remote** y **noremote**.

Notrace

Utilice el mandato **notrace** para detener la visualización de los sucesos de rastreo seleccionados en la supervisión.

Sintaxis:

```
notrace          event . . .  
                  group . . .  
                  range . . .  
                  subsystem . . .
```

event *subsistema.númerosuceso*

Suprime la visualización del suceso de rastreo especificado.

group *nombregrupo*

Suprime la visualización de sucesos de rastreo relacionados con el grupo especificado (*nombregrupo*).

range *nombresubsistema número_primer_suceso número_último_suceso*

Donde *número_primer_suceso* es el número del primer suceso del rango de sucesos especificado y *número_último_suceso* es el número del último suceso del rango de sucesos especificado.

Inhabilita el envío de datos de rastreo de paquetes para un rango de mensajes para el subsistema especificado.

Ejemplo:

```
notrace range gw 19 22
```

Suprime el envío de datos de rastreo de paquetes para los sucesos gw.19, gw.20, gw.21 y gw.22.

subsystem *nombresubsistema [nivel-anotación-cronológica]*

Suprime la visualización de sucesos de rastreo que están asociados con el subsistema y nivel de anotación cronológica especificados. Si no especifica ningún *nivel-anotación-cronológica* se suprime el rastreo de todos los niveles de anotación cronológica para el subsistema.

Ejemplo:

```
notrace subsystem fr1 error
```

```
notrace subsystem fr1
```

Notrap

Utilice el mandato **notrap** para seleccionar y desactivar mensajes de modo que ya no se envíen a la estación de trabajo de gestión de la red en detecciones SNMP.

Sintaxis:

```
notrap          event . . .
```

Mandatos de supervisión ELS (Talk 5)

group . . .
range . . .
subsystem . . .

event *subsistema.númerosuceso*

Suprime el envío del mensaje especificado en una detección SNMP (*subsistema.númerosuceso*).

group *nombregrupo*

Suprime el envío de mensajes en detecciones SNMP que se han añadido previamente al grupo especificado (*nombregrupo*).

range *nombresubsistema número_primer_suceso número_último_suceso*

Donde *número_primer_suceso* es el número del primer suceso del rango de sucesos especificado y *número_último_suceso* es el número del último suceso del rango de sucesos especificado.

Suprime el envío de mensajes para los sucesos del rango especificado para el subsistema especificado en detecciones SNMP.

Ejemplo:

```
notrap range gw 19 22
```

Suprime el envío de mensajes para los sucesos gw.19, gw.20, gw.21 y gw.22 en detecciones SNMP.

subsystem *nombresubsistema [nivel- anotación-cronológica]*

Suprime el envío de mensajes en detecciones SNMP que están asociadas con el subsistema y nivel de anotación cronológica especificados. Si no especifica ningún *nivel- anotación-cronológica* se suprimen las detecciones para todos los niveles de anotación cronológica del subsistema.

Ejemplo:

```
notrap subsystem eth error
```

Packet Trace

Utilice el mandato **packet-trace** para visualizar/habilitar/inhabilitar la información de rastreo de paquetes para varios subsistemas.

Sintaxis:

packet-trace

Utilice el mandato **Exit** cuando haya terminado de utilizar el Rastreo de paquetes.

Para descripciones de mandatos completas, consulte la sección “Mandatos de supervisión de rastreo de paquetes” en la página 201.

Remote

Utilice el mandato **remote** para seleccionar los sucesos que se han de anotar cronológicamente en un archivo remoto por el número de suceso, rango de sucesos, grupo o subsistema.

Sintaxis:

remote event . . .
group . . .

Mandatos de supervisión ELS (Talk 5)

`_range . . .`

`_subsystem . . .`

event *subsistema.númerosuceso recurso_ anotación_cronológica_sistema nivel_ anotación_cronológica_sistema*

Hace que el suceso especificado se anote cronológicamente de forma remota. El daemon de anotación cronológica del sistema utiliza los valores de recurso y de nivel de anotación cronológica del sistema en la estación de trabajo remota para determinar dónde tiene que anotar cronológicamente los mensajes. Este valor prevalece sobre los valores por omisión que se establecen con los mandatos **set facility** y **set level**.

recurso_ anotación_cronológica_sistema

log_auth
log_authpriv
log_cron
log_daemon
log_kern
log_lpr
log_mail
log_news
log_syslog
log_user
log_uucp
log_local0-7

nivel_ anotación_cronológica_sistema

log_emerg
log_alert
log_crit
log_err
log_warning
log_notice
log_info
log_debug

Estos valores NO tienen ninguna asociación particular con ningún daemon de IBM 2216. Solamente son identificadores que el daemon de anotación cronológica del sistema utiliza en la estación de trabajo remota.

Ejemplo:

```
remote event gw.019 log_user log_info
```

group *nombre_grupo recurso_ anotación_cronológica_sistema nivel_ anotación_cronológica_sistema*

Permite que los sucesos que pertenecen al grupo especificado se anoten cronológicamente de forma remota basándose en los valores de *recurso_ anotación_cronológica_sistema* y *nivel_ anotación_cronológica_sistema*. Consulte "el mandato remote event".

range *nombresubsystem número_primer_suceso número_último_suceso recurso_ anotación_cronológica_sistema nivel_ anotación_cronológica_sistema*

Mandatos de supervisión ELS (Talk 5)

Donde *número_primer_suceso* es el número del primer suceso del rango de sucesos especificado y *número_último_suceso* es el número del último suceso del rango de sucesos especificado.

Hace que los sucesos del rango especificado para el subsistema especificado se anoten cronológicamente de forma remota en el *recurso_ anotación_cronológica_sistema* y *nivel_ anotación_cronológica_sistema*. Consulte “el mandato remote event” en la página 189.

Ejemplo:

```
remote range gw 19 22 log_user log_info
```

Hace que se anoten cronológicamente los sucesos gw.19, gw.20, gw.21 y gw.22 en los archivos especificados por el valor *recurso_ anotación_cronológica_sistema* de log_user y el valor *nivel_ anotación_cronológica_sistema* de log_info.

subsystem *nombre.subsistema nivel_mensaje*
recurso_ anotación_cronológica_sistema nivel_ anotación_cronológica_sistema
Donde *nombre.subsistema* es el nombre del subsistema y *nivel_mensaje* es el nivel de los mensajes seleccionados del subsistema.

Hace que los sucesos del *nombre.subsistema* especificado cuyo *nivel_mensaje* concuerde con el *nivel_mensaje* especificado se anoten cronológicamente de forma remota basándose en el *recurso_ anotación_cronológica_sistema* y *nivel_ anotación_cronológica_sistema*. Consulte “el mandato remote event” en la página 189.

Nivel_mensaje es un valor como, por ejemplo, ALL, ERROR, INFO o TRACE. Consulte la sección “Nivel de anotación cronológica” en la página 139. El valor especificado en el mandato **remote** debe concordar con el valor codificado en el suceso en particular del subsistema, o si no el suceso del subsistema no se anotará cronológicamente de forma remota.

Ejemplo:

```
remote subsystem eth all log_user log_info
```

En el ejemplo anterior, todos los mensajes del subsistema TKR (“todos” incluye cualquier mensaje codificado para “error,” “info” o “trace”) se anotarán cronológicamente de forma remota en los archivos especificados por log_user y log_info en el sistema principal remoto.

Utilice los mandatos **list event** y **list active** para verificar lo que ha establecido con los mandatos **remote** y **noremote**.

Remove

Utilice el mandato **remove** para liberar memoria borrando la información almacenada. Si, con anterioridad, ha guardado la configuración actual con el mandato **save**, la eliminación le permite borrar la configuración guardada.

Sintaxis:

remove

Restore

Utilice el mandato **restore** para borrar todos los valores actuales (excepto los contadores) y volver a cargar la configuración ELS inicial. Para retener los valores actuales, utilice el mandato **save** antes de restaurar la configuración inicial.

Sintaxis:

restore

Retrieve

Utilice el mandato **retrieve** para volver a cargar la configuración ELS guardada. Si ha guardado previamente la configuración actual con el mandato **save**, utilice **retrieve** para volverla a cargar. **Retrieve** no borra la configuración guardada después de ejecutarse. Para borrar la configuración guardada, utilice el mandato **remove**.

Sintaxis:

retrieve

Save

Utilice el mandato **save** para almacenar la configuración actual (excepto los contadores). **Save** no afecta a la configuración por omisión (la que ha establecido con los mandatos de configuración). Utilice **save** después de modificar la configuración con los mandatos de supervisión con la intención de guardar esta configuración para después de un reinicio. Sólo puede haber una configuración guardada cada vez. Para volver a cargar la configuración guardada, utilice el mandato **retrieve**.

Sintaxis:

save

Set

Utilice el mandato **set** para establecer el número máximo de detecciones por segundo, para establecer la característica de indicación de la hora o para establecer las opciones de rastreo.

Sintaxis:

```
set                pin . . .
                   _remote-logging . . .
                   _timestamp . . .
                   trace . . .
```

pin Utilice el mandato **set pin** para establecer el parámetro pin en el número máximo de detecciones que pueden enviarse por segundo. Internamente, pin se restablece cada décima de segundo. (Una décima parte del número *detecciones_máx* se envía cada décima de segundo.)

remote-logging

Utilice el mandato **set remote-logging** para configurar las opciones de anotación cronológica remota. Cuando estas opciones se configuran desde

Mandatos de supervisión ELS (Talk 5)

el entorno de supervisión, los cambios surten efecto inmediatamente y vuelven a sus valores configurados previamente cuando se reanuda el dispositivo.

Sintaxis:

```
set remote-logging      on
                          off
                          facility . . .
                          level . . .
                          local_id
                          remote_ip_addr . . .
                          source_ip_addr ...
```

- on** Activa la anotación cronológica remota. Ahora la anotación cronológica remota está habilitada para permitir que cualquier mensaje seleccionado por el mandato **remote** se anote cronológicamente de manera activa.
- off** Desactiva la anotación cronológica remota. Se impedirá la anotación cronológica de todos los mensajes seleccionados por el mandato **remote**.

facility

Especifica un valor que, en combinación con el valor de *nivel*, se utiliza por el daemon de la anotación cronológica del sistema en la estación de trabajo remota para determinar dónde se anotan cronológicamente los mensajes. Este valor se utiliza para todos los mensajes ELS anotados cronológicamente de forma remota a menos que especifique un valor diferente para un suceso ELS, rango, grupo o subsistema en particular con el mandato **remote**.

Estos son todos los posibles valores de recurso de anotaciones cronológicas del sistema:

- log_auth
- log_authpriv
- log_cron
- log_daemon
- log_kern
- log_lpr
- log_mail
- log_news
- log_syslog
- log_user
- log_uucp
- log_local0-7

- level** Especifica un valor que, junto con el valor de *recurso*, utiliza el daemon de la anotación cronológica del sistema en la estación de trabajo remota para determinar dónde se han de anotar los mensajes. Este valor se utiliza para todos los mensajes ELS anotados cronológicamente de forma remota a menos que

Mandatos de supervisión ELS (Talk 5)

especifique un valor diferente para un suceso ELS, rango, grupo o subsistema en particular con el mandato **remote**.

Estos son todos los valores posibles de nivel de anotación cronológica del sistema:

- log_emerg
- log_alert
- log_crit
- log_err
- log_warning
- log_notice
- log_info
- log_debug

local_id

Especifica un identificador de 1 a 32 caracteres que aparece en el mensaje de anotación cronológica remota que puede utilizar para identificar la máquina que ha anotado cronológicamente un mensaje en particular.

remote_ip_addr

Se trata de una dirección IP del sistema principal remoto donde residen los archivos de anotación cronológica.

source_ip_addr

Especifica la dirección IP de la máquina que ha originado el mensaje que se está anotando cronológicamente de forma remota.

Debe utilizar una dirección IP que esté configurada en el 2216 para una identificación más fácil cuando aparece la dirección IP o el nombre de sistema principal en el mensaje ELS anotado cronológicamente de forma remota. También debe verificar que el servidor de nombres resuelva rápidamente esta dirección IP en un nombre de sistema principal, o que al menos el servidor de nombres responda rápidamente con un mensaje de “dirección no encontrada.”

Para determinar que la dirección IP se resuelve correctamente entre el mandato **host** en la estación de trabajo tal como se muestra:

```
workstation>host 5.1.1.1
host: address 5.1.1.1 NOT FOUND
workstation>
```

Si la respuesta tarda más de 1 segundo, seleccione una dirección IP que se resuelva más rápidamente.

timestamp

Le permite activar la indicación de la hora para que aparezca la hora del día o el tiempo de activación (las horas, minutos y segundos, sin fecha, desde la última vez que se ha inicializado el dispositivo) junto a cada mensaje o para desactivar la indicación de la hora.

Nota: Si activa la indicación de la hora, recuerde volver al proceso CONFIG y establecer la fecha y la hora del dispositivo utilizando el mandato time. De lo contrario, todos los mensajes aparecerán con 00:00:00, o números negativos en las horas, minutos y/o segundos, por ejemplo, 00:-4:-5.

Mandatos de supervisión ELS (Talk 5)

Utilice el mandato **set timestamp** para habilitar una de las siguientes opciones de la indicación de la hora:

timeofday

Añade el prefijo HH:MM:SS a cada mensaje ELS indicando la hora de aparición con el formato de 24 horas.

uptime

Añade el prefijo HH:MM:SS a cada mensaje ELS indicando la hora de la aparición durante un ciclo de 100 horas de tiempo de activación del dispositivo. Después de 100 horas de tiempo de activación, el contador de tiempo de activación vuelve a cero para empezar otro ciclo de 100 horas.

off Desactiva el prefijo de indicación de la hora ELS.

Sintaxis:

set timestamp [timeofday o uptime u off]

trace Utilice el mandato **set trace** para configurar las opciones de rastreo. Cuando las opciones de rastreo se configuran desde el entorno de supervisión, los cambios surten efecto inmediatamente y vuelven a sus valores configurados previamente cuando se reanuda el dispositivo.

Sintaxis:

set trace decode . . .
default-bytes-per-pkt . . .
disk-shadowing . . .
max-bytes-per-pkt . . .
memory-trace-buffer-size . . .
off
on
reset
stop-event . . .
wrap-mode . . .

decode . . .

Establece las opciones de decodificación de paquetes. No todos los componentes soportan la decodificación de paquetes.

exclude

Excluye el tipo de trama especificada para la decodificación. Los tipos de trama que se pueden excluir son:

lecontrol

LE Control

ip IP

arp ARP

ipx IPX

netbios

NetBIOS

Mandatos de supervisión ELS (Talk 5)

bpdu BPDU

appletalk

AppleTalk

aarp AppleTalk ARP

hex Desactiva la impresión de datos de tramas hexadecimales.

summary

Desactiva la impresión de una decodificación resumen en línea. Se imprime una decodificación completa.

all Excluye todos los tipos de paquetes del rastreo. No se decodifica ningún tipo de trama.

none No excluye ningún tipo de paquete del rastreo. *exlcude all.*

include

Incluye el tipo de trama especificada para la decodificación. Los tipos de trama que se pueden incluir son:

lecontrol

LE Control

ip IP

arp ARP

ipx IPX

netbios

NetBIOS

bpdu BPDU

appletalk

AppleTalk

aarp AppleTalk ARP

hex Activa la impresión de datos de tramas hexadecimales.

summary

Activa la impresión de una decodificación resumen en línea. No se imprime una decodificación completa.

all Incluye todos los tipos de paquetes del rastreo.

none No incluye ningún tipo de paquete en el rastreo. Es contrario a *include all*.

off Desactiva la decodificación.

on Activa la codificación.

Nota: El valor por omisión es imprimir una salida de decodificación completa para todos los tipos de trama. Utilice el mandato **list trace-status** para ver los valores de decodificación actuales. Consulte la página 185.

Mandatos de supervisión ELS (Talk 5)

default-bytes-per-pkt *bytes*

Establece el número por omisión de bytes rastreados. Este valor se utiliza si el componente que efectúa el rastreo no especifica ningún valor.

disk-shadowing **[[off u on] o [delete-file o tamaño-registro o límite-tiempo]]**

Activa y desactiva la copia continua en disco, establece el tamaño máximo de archivo de rastreo o establece el tiempo máximo para los rastreos con copia continua en disco.

[off u on]

Activa o desactiva la copia continua en disco. Si la copia continua en disco está habilitada, los registros de rastreo se copian en el disco duro. Una vez copiado un registro de rastreo en el disco duro, ya no se puede visualizar desde la supervisión.

Nota: La copia continua en disco debe establecerse en OFF siempre que se emitan los mandatos de software WRITE, TFTP software, RETRIEVE system dump o COPY.

Activa o desactiva la copia continua en disco y establece el tamaño máximo del archivo de rastreo. Si la copia continua en disco está habilitada, los registros de rastreo se copian en el disco duro. Una vez copiado un registro de rastreo en el disco duro, ya no se puede visualizar mediante la supervisión.

record-size *bytes*

Establece el tamaño de registro para los registros del archivo de rastreo:

Valores válidos:

1024, 2048 ó 4096 bytes

Por omisión: 2048 bytes

Notas:

1. Si ya existe un archivo de rastreo, se visualiza "Cannot change Record Size without first deleting the existing Trace File" y no se cambia el tamaño de registro.
2. Si configura un tamaño de registro y ya existe un archivo de rastreo, el rastreo utilizará el tamaño de registro del archivo existente.

delete-file

Suprime el archivo de rastreo (sólo en el subdirectorio asociado con el banco activo).

Nota: Si la copia continua en disco está activada cuando se emite el mandato, se visualiza "Disk-shadowing must be set to OFF before trace file can be deleted" y no se suprime el archivo.

time-limit *horas*

Establece el tiempo máximo para la copia continua en disco de los rastreos:

Mandatos de supervisión ELS (Talk 5)

Valores válidos:

De 1 a 72 horas

Valor por omisión

24

Nota: Se detiene la copia continua en disco (el rastreo continúa) después de que transcurra este tiempo. El tiempo real se restablece en 0 cuando se vuelve a activar la copia continua en disco.

max-bytes-per-pkt *bytes*

Establece el número máximo de bytes rastreados para cada paquete.

memory-trace-buffer-size *bytes*

Establece el tamaño, en bytes, del almacenamiento intermedio de rastreo de RAM.

Valores válidos: 0, ≥ 10.000

Valor por omisión: 0

off Inhabilita el rastreo de paquetes.

on Habilita el rastreo de paquetes.

reset Borra el almacenamiento intermedio de rastreo y restablece todos los contadores asociados.

stop-event *id suceso*

Detiene el rastreo cuando se produce un suceso (id suceso). Entre un id de suceso ELS (por ejemplo: TCP.013) o "Ninguno". "Ninguno" es el valor por omisión. El rastreo sólo se detiene si está habilitada la visualización del suceso ELS en particular.

Cuando se produce un suceso de detención, se graba una entrada en el almacenamiento intermedio de rastreo. El mandato **view** para esta entrada de rastreo visualizará " Tracing stopped due to ELS Event Id: TCP.013".

Después de que se detenga el rastreo debido a un suceso de detención, debe volver a habilitar el rastreo con el mandato **set trace on**. (Un reinicio también volverá a habilitar el rastreo si se ha habilitado desde el indicador ELS Config>.)

Ejemplo:

```
set trace stop-event TCP.013
```

wrap-mode *off/on*

Activa y desactiva la modalidad de reinicio del almacenamiento intermedio de rastreo. Cuando la modalidad de reinicio está habilitada y el almacenamiento intermedio de rastreo está lleno, se grabarán los nuevos registros de rastreo encima de los registros de rastreo anteriores cuando sea necesario para continuar el rastreo.

Statistics

Utilice el mandato **statistics** para visualizar una lista de todos los subsistemas disponibles y sus estadísticas.

Mandatos de supervisión ELS (Talk 5)

Nota: El ejemplo siguiente puede no coincidir exactamente con su pantalla. La salida del mandato depende de la versión y el release del software instalado.

Sintaxis:

statistics

Ejemplo:

statistics

Subsys	Vector	Exist	String	Active	Heap
GW	105	101	3411	0	0
FLT	20	7	184	0	0
BRS	50	5	201	0	0
ARP	150	142	7030	0	0
IP	100	100	2463	2	20
ICMP	30	21	529	0	0
TCP	60	57	2420	0	0
UDP	10	6	179	0	0
BTP	40	13	695	0	0
RIP	30	22	474	0	0
OSPF	80	73	2859	0	0
MSPF	40	17	593	0	0
TFTP	35	29	819	0	0
SNMP	30	28	821	0	0
DVM	30	21	589	0	0
DN	140	115	5842	0	0
XN	35	21	780	0	0
IPX	110	110	4705	0	0
CLNP	80	58	1763	0	0
ESIS	40	24	716	0	0
ISIS	80	58	2422	0	0
DNAV	50	26	1314	0	0
AP2	80	70	1755	0	0
ZIP2	60	51	1859	0	0
R2MP	50	38	1185	0	0
VIN	90	79	3159	0	0
SRT	120	94	5040	0	0
STP	60	32	1590	0	0
BR	50	30	1616	0	0
SRLY	30	28	1409	0	0
ETH	60	47	1098	0	0
SL	50	35	584	0	0
TKR	60	45	2031	0	0
X25	70	53	1909	0	0
FDDI	30	27	1155	0	0
SDLC	100	95	4263	0	0
FRL	130	97	6068	0	0
PPP	190	186	6394	0	0
X251	50	16	546	0	0
X252	50	34	996	0	0
X253	50	42	1649	0	0
ISDN	50	43	1994	0	0
IPPN	20	4	132	0	0
WRS	40	33	1938	0	0
LNМ	70	60	3137	0	0
LLC	170	168	9840	0	0
BGP	80	74	2477	0	0
MCF	15	9	244	0	0
DLS	500	497	24340	0	0
V25B	30	28	1058	0	0
BAN	30	29	1223	0	0
COMP	80	26	1050	0	0
NBS	100	50	3029	0	0
ATM	300	216	10808	0	0
LEC	200	174	7258	0	0
APPN	100	28	467	0	0
ILMI	150	23	487	0	0
SAAL	30	26	621	0	0
SVC	30	26	465	0	0
LES	400	361	22333	0	0
LECS	150	145	5666	0	0

Mandatos de supervisión ELS (Talk 5)

EVLOG	1	1	105	0	0
NOT	25	15	508	0	0
NHRP	250	211	8193	0	0
XTP	64	58	2271	0	0
ESC	150	67	3122	0	0
LCS	40	22	858	0	0
LSA	70	61	3506	0	0
MPC	130	30	1677	3	44
SCSP	40	34	1234	0	0
ALLC	50	36	1842	0	0
NDR	50	38	1150	0	0
MLP	100	93	4006	0	0
SEC	50	30	688	0	0
ENCR	100	4	194	0	0
PM	25	6	120	0	0
DGW	20	9	238	0	0
QLLC	55	54	2411	0	0
Total	6490	4942	215805	5	64

Maximum:7976 vector, 155 subsystem

Memory:71784/620 vector+ 81256/217714 data+ 64 heap=371438Subsys

Subsys

Nombre del subsistema

Vector

Tamaño máximo del subsistema

Exist Número de sucesos definidos en este subsistema

String Número de bytes utilizados para el almacenamiento de mensajes en este subsistema

Active Número de sucesos activos (visualizados, de detección o contados) del subsistema

Heap Memoria dinámica que utiliza el subsistema

Trace

Utilice el mandato **trace** para seleccionar los sucesos de rastreo que se han de visualizar en la supervisión del sistema. Este mandato proporciona una función similar al mandato **packet trace** descrito en la sección “Mandatos de supervisión de rastreo de paquetes” en la página 201.

Sintaxis:

```
trace                event . . .  
                        group . . .  
                        range . . .  
                        subsystem . . .
```

event *subsistema.númerosuceso*

Hace que se visualice el suceso de rastreo especificado (*subsistema.númerosuceso*) en la supervisión del sistema.

group *nombregrupo*

Permite visualizar los sucesos de rastreo que se han añadido previamente al grupo especificado, en el dispositivo que supervisa.

range *nombresubsistema número_primer_suceso número_último_suceso*

Mandatos de supervisión ELS (Talk 5)

Donde *número_primer_suceso* es el número del primer suceso del rango de sucesos especificado y *número_último_suceso* es el número del último suceso del rango de sucesos especificado.

Hace que se visualicen los sucesos de rastreo del rango especificado para el subsistema especificado, en la supervisión del sistema.

Ejemplo:

```
trace range gw 19 22
```

Hace que se visualicen los sucesos de rastreo gw.19, gw.20, gw.21 y gw.22 en la supervisión del sistema.

subsystem *nombresubsistema*

Permite visualizar los sucesos de rastreo asociados con el subsistema especificado en el dispositivo que supervisa.

Trap

Utilice el mandato **trap** para seleccionar el mensaje que se ha de enviar a la estación de trabajo de gestión de la red SNMP remota. Una estación de trabajo de gestión de la red SNMP remota es un sistema principal IP que actúa como un gestor SNMP.

Sintaxis:

```
trap                event . . .  
                    group . . .  
                    range . . .  
                    subsystem . . .
```

event *subsistema.númerosuceso*

Hace que el mensaje especificado (*subsistema.númerosuceso*) se envíe a la estación de trabajo de gestión de la red en una detección SNMP.

group *nombregrupo*

Permite enviar los mensajes, que se han añadido previamente al grupo especificado, a una estación de trabajo de gestión de la red en una detección SNMP.

range *nombresubsistema número_primer_suceso número_último_suceso*

Donde *número_primer_suceso* es el número del primer suceso del rango de sucesos especificado y *número_último_suceso* es el número del último suceso del rango de sucesos especificado.

Hace que se envíen los mensajes, que están en el rango especificado para el subsistema especificado, a una estación de trabajo de gestión de la red en una detección SNMP.

Ejemplo:

```
trap range gw 19 22
```

Hace que se envíen los mensajes de los sucesos gw.19, gw.20, gw.21 y gw.22 a una estación de trabajo de gestión de la red en una detección SNMP.

subsystem *nombresubsistema*

Permite que se envíen los mensajes asociados con el subsistema especificado a una estación de gestión en una detección SNMP.

Mandatos de supervisión ELS (Talk 5)

Nota: Los mensajes para los subsistemas IP ICMP, ARP y UDP no pueden enviarse en detecciones SNMP porque estas áreas se utilizan, o pueden utilizarse, en el proceso de envío de la detección SNMP. Esto podría conducir a un bucle infinito de tráfico haciendo que el dispositivo tuviese que realizar un esfuerzo indebido.

View

Utilice el mandato **view** para ver los paquetes rastreados.

Sintaxis:

```
view                current
                    first
                    jump
                    last
                    next
                    prev
                    search ...
```

current

Visualiza el paquete de rastreo actual. Si el paquete actual no es válido, se visualiza el primer paquete del almacenamiento intermedio de rastreo.

first Visualiza el primer paquete rastreado del almacenamiento intermedio de rastreo.

jump *n*

Visualiza el paquete rastreado *n* antes o después del paquete actual.

last Visualiza el último paquete rastreado del almacenamiento intermedio de paquetes.

next Visualiza el siguiente paquete rastreado.

prev Visualiza el anterior paquete rastreado.

search

Visualiza el siguiente paquete rastreado que contiene la información especificada. Puede especificar la información de búsqueda como:

- Serie hexadecimal
- Dirección IP
- Texto ASCII

Mandatos de supervisión de rastreo de paquetes

Esta sección describe los mandatos de la Supervisión de rastreo de paquetes. Después de acceder al entorno de Supervisión de rastreo de paquetes, puede entrar los mandatos de Supervisión de rastreo de paquetes en el indicador ELS Packet Trace>.

Tabla 19. Resumen de los mandatos de supervisión de rastreo de paquetes

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado "Cómo obtener ayuda" en la página 10.
Off	Inhabilita el rastreo de paquetes.

Mandatos de supervisión ELS (Talk 5)

Tabla 19. Resumen de los mandatos de supervisión de rastreo de paquetes (continuación)

Mandato	Función
On	Habilita el rastreo de paquetes. Solicita el tamaño de almacenamiento intermedio de rastreo de memoria si no se ha establecido anteriormente.
Reset	Borra el almacenamiento intermedio de rastreo y restablece todos los contadores asociados.
Set	Configura las opciones de rastreo.
Subsystems	Activa el rastreo para los subsistemas que soportan el rastreo de paquetes o visualiza un resumen.
Trace-status	Visualiza información sobre el estado del rastreo de paquetes, incluyendo la configuración y el tiempo de ejecución.
View	Proporciona la visualización de la consola de almacenamientos intermedios de rastreo de paquetes capturados
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página 11.

Off

Utilice el mandato **off** para inhabilitar el rastreo de paquetes.

Sintaxis:

off

On

Utilice el mandato **on** para habilitar el rastreo de paquetes.

Sintaxis:

on

Reset

Utilice el mandato **reset** para borrar el almacenamiento intermedio de rastreo y restablecer todos los contadores asociados.

Sintaxis:

reset

Set

Utilice el mandato **set** para configurar las opciones de rastreo.

Sintaxis:

set

decode

default-bytes-per-pkt

disk-shadowing

max-bytes-per-pkt

memory-trace-buffer-size

stop-event

wrap-mode

exit

Para ver una explicación del mandato **set**, consulte la página 194.

Subsystems

Utilice el mandato **subsystems** para activar el rastreo para los subsistemas que soportan el rastreo de paquetes o para visualizar un resumen.

Sintaxis:

```
subsystems          atm
                    fddi
                    lec
                    summary
```

Ejemplo:

```
subsystems atm
Network number? 0
ATM Interface is selected
on | off | list [list]? on
Note that SVC uses VPI = 0, VCI = 5
and ILMI uses VPI = 0, VCI = 16
Beginning of VPI range [0]?
End of VPI range [0]?
Beginning of VCI range [0]? 16
End of VCI range [0]? 16
Tracing event ATM.88: ATM frames
```

Ejemplo:

```
subsystems lec
Network number? 1
ATM Emulated LAN is selected
on | off | list [list]? on
Trace which types of frames (data, control, both) [both]?
Tracing event LEC.11: data frames over ATM Forum LEC: interface 1
Tracing event LEC.12: control frames over ATM Forum LEC: interface 1
Note that if the user DISABLEs and TESTs this LEC interface,
the LEC trace settings from Talk 6 Config will take effect.
```

MAC Address packet filtering can be enabled under the LEC net using the 'trace mac-address' command.

Ejemplo:

```
subsystems summary
Subsystems Being Traced

ATM      net number = 0, VPI Range:    0 -    0
          VCI Range:    16 -   16
LEC      net number = 1
```

Trace-Status

Utilice el mandato **trace-status** para obtener información actualizada relativa al rastreo de paquetes.

Sintaxis:

```
trace-status
```

Ejemplo:

```
trace-status
----- Configuration -----
Trace Status:OFF  Wrap Mode:OFF  Decode Packets:OFF  HD Shadowing:OFF
RAM Trace Buffer Size:0  Maximum Trace Buffer File Size:10000000
Max Packet Bytes Trace:256  Default Packet Bytes Traced:100
Trace File Record Size:2048  Stop Trace Event: None
Maximum Hours to HD Shadow: 24
----- Run-time Status -----
Packets in RAM Trace Buffer:0  Free Trace Buffer Memory:0
```

Mandatos de supervisión ELS (Talk 5)

```
Trace Errors:0 First Packet:0 Last Packet:0
Trace Records Stored on HD:0 Trace Buffer File Size:0
HD-Shadowing Time Exceeded? NO
Has Stop Trace Event Occurred? NO
```

View

Utilice el mandato **view** para entrar en la visualización de la supervisión de almacenamientos intermedios de rastreo de paquetes capturados.

Para ver una explicación de los mandatos **view**, consulte la sección “View” en la página 201.

Sintaxis:

```
view                current
                    first
                    jump
                    last
                    next
                    prev
                    search
                    exit
```

Mandatos de la supervisión de filtros de red ELS

Esta sección explica los mandatos para manipular los filtros de red ELS. Para entrar en el entorno de filtros, entre el mandato **filter net** en el indicador ELS>. Entre los mandatos de supervisión en el indicador ELS Filter net>.

Tabla 20. Mandatos de la supervisión de filtros de red ELS

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página 10.
Create	Crea un filtro y le asigna un número. Están permitidos un máximo de 64 filtros.
Delete	Suprime un número de filtro especificado o todos los filtros.
Disable	Inhabilita un número de filtro especificado o todos los filtros.
Enable	Habilita un número de filtro especificado o todos los filtros.
List	Lista un número de filtro especificado o todos los filtros.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página 11.

Create

Utilice el mandato **create** para crear un filtro de red ELS.

Sintaxis:

```
create cola                event nombre_suceso númerored_inicio
                               númerored_final

                               range rango_sucesos númerored_inicio
                               númerored_final

                               subsystem nombre_subsistema númerored_inicio
                               númerored_final
```

Mandatos de supervisión ELS (Talk 5)

cola La cola para la que establece el filtro. Las colas válidas son:
Visualización
Rastreo
Detección
Remota

event *nombre_suceso número_red_inicio número_red_final*

Especifica el suceso y los números de red que está filtrando.

Si especifica el mismo número para *inicio_red#* y *final_red#*, está filtrando un solo número de red.

El mandato **create trap event GW.009 2 10** filtra las detecciones para el mensaje GW.009 para los números de red del 2 al 10.

range *rango_sucesos número_red_inicio número_red_final*

Especifica el rango de mensajes ELS y números de red que está filtrando.

Si especifica el mismo número para *inicio_red#* y *final_red#*, está filtrando un solo número de red.

El mandato **create remote range ipx 19 22 3 6** filtra todos los mensajes ipx empezando por IPX.019 y finalizando en IPX.022 para los números de red del 3 al 6 para la anotación cronológica remota.

subsystem *nombre_subsistema número_red_inicio número_red_final*

Especifica el subsistema y los números de red que está filtrando.

Si especifica el mismo número para *inicio_red#* y *final_red#*, está filtrando un solo número de red.

El mandato **create display subsys ip 1 1**, filtra todos los mensajes ELS para el subsistema ip que contiene el número de red 1 para su visualización. Se descartan todos los demás mensajes del subsistema ip.

Delete

Utilice el mandato **delete** para suprimir un filtro ELS específico o todos los filtros ELS.

Sintaxis:

```
delete                all  
                        filter númerofiltro
```

all Suprime todos los filtros configurados actualmente.

filter *númerofiltro*

Suprime el filtro especificado por *númerofiltro*. Utilice el mandato **list** para obtener el número del filtro que desea suprimir.

Disable

Utilice el mandato **disable** para inhabilitar un filtro ELS específico o todos los filtros ELS.

Sintaxis:

```
disable              all  
                        filter númerofiltro
```

all Inhabilita todos los filtros configurados actualmente.

Mandatos de supervisión ELS (Talk 5)

filter *númerofiltro*

Inhabilita el filtro especificado por *númerofiltro*. Utilice el mandato **list** para obtener el número del filtro que desea inhabilitar.

Enable

Utilice el mandato **enable** para habilitar un filtro ELS específico o todos los filtros ELS.

Sintaxis:

```
enable                all
                        filter númerofiltro
```

all Habilita todos los filtros configurados actualmente.

filter *númerofiltro*

Habilita el filtro especificado por *númerofiltro*. Utilice el mandato **list** para obtener el número del filtro que desea habilitar.

List

Utilice el mandato **list** para listar un filtro ELS específico o todos los filtros ELS.

Sintaxis:

```
list                  all
                        filter númerofiltro
```

all Lista todos los filtros configurados actualmente.

filter *númerofiltro*

Lista el filtro especificado por *númerofiltro*.

Mandatos de la supervisión de almacenamientos intermedios de mensajes ELS

La Tabla 21 describe los mandatos disponibles en el indicador ELS Config Advanced>.

Tabla 21. Mandatos de la supervisión de almacenamientos intermedios de mensajes ELS

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado "Cómo obtener ayuda" en la página 10.
Flush	Borra el almacenamiento intermedio de mensajes y desactiva la anotación cronológica para el almacenamiento intermedio de mensajes.
List	Visualiza los valores operativos para el almacenamiento intermedio de mensajes.
Log	Habilita la anotación cronológica de los mensajes seleccionados en el almacenamiento intermedio de mensajes.
Nolog	Desactiva la anotación cronológica de los mensajes seleccionados en el almacenamiento intermedio de mensajes.
Read-file	Lee un almacenamiento intermedio de mensajes formateado de un archivo y lo visualiza en la consola.

Mandatos de supervisión ELS (Talk 5)

Tabla 21. Mandatos de la supervisión de almacenamientos intermedios de mensajes ELS (continuación)

Mandato	Función
Set	Establece el tamaño del almacenamiento intermedio de mensajes, la modalidad de reinicio, cuándo se produce la anotación cronológica, qué suceso finalizará el almacenamiento intermedio de mensajes y lo que hace el sistema cuando se detiene el almacenamiento intermedio por un suceso.
Tftp	Envía el almacenamiento intermedio de mensajes ELS a un archivo de un sistema principal remoto.
View	Visualiza todos o un número específico de mensajes del almacenamiento intermedio de mensajes. También puede controlar la forma en que los mensajes se desplazan fuera de la pantalla.
Write-buffer	Graba el almacenamiento intermedio de mensajes ELS en la unidad de disco duro. El almacenamiento intermedio se formatea antes de grabarse. El nombre de archivo de la unidad de disco duro es siempre ELSADV.LOG.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página 11.

Flush

Utilice el mandato **flush** para desactivar la anotación cronológica, borrar los mensajes del almacenamiento intermedio y liberar memoria de almacenamiento intermedio para que el sistema la utilice para otro fin.

Sintaxis:

flush buffer

List

Utilice el mandato **list** para listar la configuración del almacenamiento intermedio de mensajes ELS.

Sintaxis:

list status

Ejemplo:

```
ELS Advanced> list status
-----Configuration-----
Logging Status:  OFF      Wrap Mode:  ON      Logging Buffer Size:  8500 Kytes
Stop-Event:     APPN.2    Stop-String:  netdn for intf 6
Additional Stop-Action: APPN DUMP
-----Run-Time Status-----
Has Stop Condition Occurred ?  YES      Messages currently in buffer:  1222
```

Consulte la sección "Set" en la página 209 para ver la descripción de los mandatos que cambian los valores de la pantalla.

Log

Utilice el mandato **log** para seleccionar los mensajes que se anotarán cronológicamente en el almacenamiento intermedio de mensajes.

Sintaxis:

log event
group

Mandatos de supervisión ELS (Talk 5)

range

subsystem

event *subsistema.númersuceso*

Hace que se anote cronológicamente el mensaje especificado (*subsistema.númersuceso*) en el almacenamiento intermedio de mensajes.

group *nombregrupo*

Permite que los mensajes que se habían añadido previamente al grupo especificado se anoten cronológicamente en el almacenamiento intermedio de mensajes.

range *nombresubsistema número_primer_suceso número_último_suceso*

Donde *número_primer_suceso* es el número del primer suceso del rango de sucesos especificado y *número_último_suceso* es el número del último suceso del rango de sucesos especificado.

Hace que los mensajes del rango especificado para el subsistema especificado se anoten cronológicamente en el almacenamiento intermedio de mensajes.

Ejemplo:

```
log range gw 19 22
```

Hace que se anoten cronológicamente los mensajes de los sucesos gw.19, gw.20, gw.21 y gw.22 en el almacenamiento intermedio de mensajes.

subsystem *nombresubsistema*

Permite que los mensajes asociados con el subsistema especificado se anoten cronológicamente en el almacenamiento intermedio de mensajes.

Nolog

Utilice el mandato **nolog** para eliminar los mensajes de la lista de mensajes definida que se anotan cronológicamente en el almacenamiento intermedio de mensajes.

Sintaxis:

nolog

event

group

range

subsystem

event *subsistema.númersuceso*

Hace que no se anote cronológicamente el mensaje especificado (*subsistema.númersuceso*) en el almacenamiento intermedio de mensajes.

group *nombregrupo*

Permite que los mensajes que se habían añadido previamente al grupo especificado no se anoten cronológicamente en el almacenamiento intermedio de mensajes.

range *nombresubsistema número_primer_suceso número_último_suceso*

Donde *número_primer_suceso* es el número del primer suceso del rango de sucesos especificado y *número_último_suceso* es el número del último suceso del rango de sucesos especificado.

Mandatos de supervisión ELS (Talk 5)

Hace que los mensajes que están en el rango especificado para el subsistema especificado no se anoten cronológicamente en el almacenamiento intermedio de mensajes.

Ejemplo:

```
log range gw 19 22
```

Hace que no se anoten cronológicamente los mensajes de los sucesos gw.19, gw.20, gw.21 y gw.22 en el almacenamiento intermedio de mensajes.

subsystem *nombresubsistema*

Permite que los mensajes asociados con el subsistema especificado no se anoten cronológicamente en el almacenamiento intermedio de mensajes.

Read-file

Utilice el mandato **read-file** para leer los mensajes ELS formateados de un archivo de la unidad de disco duro , ELSADV.LOG, creado por el mandato **write-buffer**.

Nota: Si entra este mandato y no hay ninguna unidad de disco duro disponible, recibirá un mensaje indicando que la unidad no está disponible.

Sintaxis:

read-file

Set

Utilice el mandato **set** para cambiar las opciones configuradas de almacenamiento intermedio de mensajes ELS.

Sintaxis:

```
set                logging [on u off]  
                    stop action . . .  
                    stop event subsistema.númerosuceso  
                    stop string texto  
                    wrap [on o off]
```

logging [on u off]

Especifica si se producirá el almacenamiento intermedio de mensajes. Este mandato no surtirá efecto hasta que asigne un almacenamiento intermedio utilizando el mandato **set buffer-size**. El valor por omisión es desactivado.

stop action [appn-dump o disk-offload o none o system-dump]

Especifica la acción adicional que el sistema efectúa cuando se produce el "suceso de detención" (y si se especifica, la "serie de detención"). Las acciones son:

appn-dump

Vuelca el protocolo APPN, si está activo. El vuelco APPN indicará que el vuelco se ha realizado como resultado de una acción de detención.

disk-offload

Graba una versión formateada del almacenamiento intermedio en un archivo de la unidad de disco duro . Si ya existe el archivo, el

Mandatos de supervisión ELS (Talk 5)

nuevo archivo lo sustituye. Después, puede utilizar el mandato de supervisión **tftp file** para enviar el archivo a un sistema principal remoto.

none No se efectúa ninguna otra acción después de detenerse la anotación cronológica.

system-dump

Vuelca todo el sistema. El vuelco del sistema indicará que se ha realizado el vuelco como resultado de una acción de detención.

Valor por omisión: none

stop event [*subsistema.númerosuceso* o **none**]

Especifica el suceso (*subsistema.númerosuceso*) que detiene la anotación cronológica. Si ha especificado una serie de detención, el texto de la serie de detención también debe coincidir. Cuando se produce el suceso de detención:

1. Si no se ha especificado ninguna acción de detención (es decir, none), se anotan cronológicamente los cinco mensajes ELS siguientes. Sin embargo, si se ha especificado una acción de detención (un valor distinto de none), no se anotan cronológicamente más mensajes ELS.
2. Se detiene la anotación cronológica.
3. El sistema realiza la “acción de detención” especificada.

La anotación cronológica permanece detenida hasta la próxima vez que se emite el mandato **set logging on** o se reanuda el dispositivo.

Si no especifica el suceso de detención cuando entra el mandato, el sistema le solicita que entre el suceso de detención. La especificación de **none** inhabilita la función del suceso de detención.

Valor por omisión: none

stop string *texto* o **none**

Especifica la serie que se ha de utilizar conjuntamente con el “suceso de detención” para detener la anotación cronológica. Si no ha especificado ningún suceso de detención, el sistema pasa por alto la “serie de detención.”

El *texto* puede ser cualquier serie ASCII de hasta 32 caracteres de longitud. Si no especifica el *texto* cuando entra el mandato, el sistema le solicitará la serie. Si se entra **none** se borra la “serie de detención.”

Valor por omisión: none

wrap [**on** u **off**]

Especifica si se ha de detener la anotación cronológica cuando el almacenamiento intermedio esté lleno (off) o si se han de anotar los nuevos mensajes al principio del almacenamiento intermedio (on).

Valor por omisión: on

Tftp

Utilice el mandato **tftp** para enviar el almacenamiento intermedio de mensajes ELS a un sistema principal remoto como un archivo formateado.

Sintaxis:

tftp buffer [formatted] *direc_ip_dest nombarch_dest*

Mandatos de supervisión ELS (Talk 5)

file direc_ip_dest nombarch_dest

buffer [formatted] *direc_ip_dest nombarch_dest*

Especifica que el almacenamiento intermedio de mensajes ELS se ha de enviar al sistema principal remoto indicado por *direc_ip_dest* como el archivo *nombarch_dest*. El almacenamiento intermedio puede estar formateado.

View

Utilice el mandato **view** para ver todos los mensajes para un número específico de mensajes del almacenamiento intermedio de mensajes.

Sintaxis:

view *all [scroll/noscroll]*
last [scroll/noscroll número]

all *scroll/noscroll*

Visualiza todos los mensajes del almacenamiento intermedio de mensajes.

[scroll]

Especifica que la pantalla se detiene temporalmente hasta que se pulsa la barra espaciadora.

Nota: Si está visualizando un gran número de mensajes, especifique **scroll** para no perderse ningún mensaje importante.

noscroll

Especifica que los mensajes se desplazarán fuera de la pantalla si el número de mensajes excede la longitud de la pantalla.

last *scroll/noscroll número*

Visualiza *número* últimos mensajes del almacenamiento intermedio de mensajes.

[scroll]

Especifica que la pantalla se detiene temporalmente después de visualizar una pantalla completa de mensajes y espera que el usuario pulse la barra espaciadora para pasar a la siguiente pantalla.

Nota: Si está visualizando un gran número de mensajes, especifique **scroll** para no perderse ningún mensaje importante.

noscroll

Especifica que los mensajes se desplazarán de forma continuada fuera de la pantalla sin ningún control de desplazamiento hasta que se hayan visualizado todos los mensajes del almacenamiento intermedio (o el último número de los mensajes pedidos).

number

Especifique un número del 1 al número total de mensajes del almacenamiento intermedio de mensajes. Para visualizar el número total de mensajes del almacenamiento intermedio, utilice el mandato de supervisión **list status**.

Mandatos de supervisión ELS (Talk 5)

Write-buffer

Utilice el mandato **write-buffer** para grabar los mensajes ELS formateados en la unidad de disco duro .

Nota: Si entra este mandato y no hay ninguna unidad de disco duro disponible, recibirá un mensaje indicando que la unidad no está disponible.

Sintaxis:

write-buffer

Capítulo 12. Configuración y supervisión del rendimiento

Este capítulo describe cómo utilizar los mandatos operativos de supervisión y configuración del rendimiento e incluye las secciones siguientes:

- “Visión general del rendimiento”
- “Exactitud de la información del rendimiento”
- “Acceso al entorno de configuración del rendimiento”
- “Mandatos de configuración del rendimiento” en la página 214
- “Acceso al entorno de supervisión del rendimiento” en la página 215
- “Mandatos de supervisión del rendimiento” en la página 215

Visión general del rendimiento

La configuración del rendimiento le permite supervisar la carga de la CPU. En el estado desocupado (carga sin trabajo), el rendimiento refleja las operaciones que el dispositivo realiza continuamente, como parte de la gestión de interfaces externas. La carga de CPU registrada en el estado desocupado depende de:

- El número de protocolos en ejecución.
- El número de interfaces/tarjetas instaladas.
- El tipo de interfaces instaladas.

La función del rendimiento se puede utilizar como una herramienta para el análisis de tendencias, la evaluación de cuellos de botella y la planificación de la capacidad. Mediante la reunión de la información de la utilización de CPU en el dispositivo, un gestor de la red puede supervisar:

- La carga de CPU según la hora.
- La carga de CPU según la ubicación del dispositivo en la red.
- La carga de CPU según la productividad de tráfico.
- La carga de CPU según la carga de usuario (por ejemplo: sesiones TN3270, marcación RDSI en clientes)

Exactitud de la información del rendimiento

Si pide un análisis del rendimiento la primera vez que el 2216 se pone en línea, verá valores que reflejan un estado de inicialización con poco o ningún tráfico de red, por lo que es de poca ayuda en el equilibrio de la carga de la red.

Es mejor utilizar los informes del rendimiento que se generan bajo cargas normales después de 2 minutos aproximadamente de funcionamiento.

Acceso al entorno de configuración del rendimiento

Utilice el procedimiento siguiente para acceder al proceso de configuración del supervisor del rendimiento.

1. En el indicador OPCON, entre **talk 6**. (Para ver los detalles de este mandato, consulte la sección “¿Qué es CONFIG?” en la página 67.) Por ejemplo:

```
* talk 6
Config>
```

Después de entrar el mandato **talk 6**, se visualiza el indicador CONFIG (Config>) en el terminal. Si no aparece el indicador cuando entre en la configuración, pulse **intro** de nuevo.

2. En el indicador CONFIG, entre el mandato **perf.** para obtener el indicador PERF Config>.

Mandatos de configuración del rendimiento

Para configurar el rendimiento, entre los mandatos en el indicador PERF Config>.

Tabla 22. Resumen de los mandatos de configuración PERF

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página 10.
Disable	Inhabilita la reunión de estadísticas de utilización de la CPU o la salida del supervisor ELS Ta1k 2.
Enable	Habilita la reunión de las estadísticas de utilización de la CPU o la salida del supervisor ELS Ta1k 2.
List	Lista la configuración.
Set	Establece el período de información.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página 11.

Disable

Utilice el mandato **disable** para inhabilitar la reunión de las estadísticas de utilización de la CPU e inhabilitar la salida del supervisor ELS ta1k 2.

Sintaxis:

disable cpu statistics
 t2 output

Enable

Utilice el mandato **enable** para habilitar la reunión de las estadísticas de utilización de la CPU y habilitar la salida del monitor ELS ta1k 2.

Sintaxis:

enable cpu statistics
 t2 output

List

Utilice el mandato **list** para visualizar la configuración del supervisor del rendimiento.

Sintaxis:

list

Set

Utilice el mandato **set** para establecer el período de información.

Sintaxis:

set *tiempo*

tiempo

Especifica el tiempo corto de ventana.

Valores válidos: De 2 a 30 segundos

Valor por omisión: 5

Acceso al entorno de supervisión del rendimiento

Utilice el procedimiento siguiente para acceder a los mandatos de supervisión del rendimiento. Este proceso le proporciona acceso al proceso de *supervisión* del rendimiento.

1. En el indicador OPCON, entre **talk 5**. (Para ver los detalles de este mandato, consulte la sección “Capítulo 8. El proceso de operación/supervisión (GWCON - Talk 5) y sus mandatos” en la página 117.) Por ejemplo:

```
* talk 5
+
```

Después de entrar el mandato **talk 5**, se visualiza el indicador GWCON (+) en el terminal. Si no aparece el indicador cuando entre en la configuración, pulse **intro** de nuevo.

2. En el indicador +, entre el mandato **perf** para obtener el indicador PERF Console>.

Ejemplo:

```
+ perf
PERF Console>
```

Mandatos de supervisión del rendimiento

Esta sección describe los mandatos de supervisión del rendimiento.

Tabla 23. Resumen de los mandatos de supervisión PERF

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página 10.
Clear	Borra las estadísticas de máxima utilización de la CPU y restablece el período de información a un nuevo ciclo.
Disable	Inhabilita la reunión de estadísticas de utilización de la CPU o la salida del supervisor ELS Talk 2.
Enable	Habilita la reunión de las estadísticas de utilización de la CPU o la salida del supervisor ELS Talk 2.
List	Lista la configuración.
Report	Visualiza un informe de las estadísticas del rendimiento.
Set	Establece el período de información.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página 11.

Disable

Utilice el mandato **disable** para inhabilitar la reunión de las estadísticas de utilización de la CPU e inhabilitar la salida del supervisor ELS talk 2.

Sintaxis:

```
disable          cpu statistics
                   t2 output
```

Enable

Utilice el mandato **enable** para habilitar la reunión de las estadísticas de utilización de la CPU y habilitar la salida del monitor ELS talk 2.

Mandatos de supervisión del rendimiento (Talk 5)

Sintaxis:

```
enable                cpu statistics  
                        t2 output
```

List

Utilice el mandato **list** para visualizar la configuración del supervisor del rendimiento.

Sintaxis:

```
list
```

Report

Utilice el mandato **report** para visualizar las estadísticas del supervisor del rendimiento.

Sintaxis:

```
report
```

Ejemplo:

```
PERF Console>report  
-----  
KEY: SW = Short Window = 9 seconds  
KEY: LW = Long Window = 9.0 minutes (60 x SW)  
  
CPU UTIL : Most recent SW                = 38%  
            Most recent LW                = 33%  
            Highest for all SW's          = 92%  
            Highest for all LW's          = 52%  
            % of time cpu util (SW) was > 60% = 16%  
            % of time cpu util (SW) was > 70% = 15%  
            % of time cpu util (SW) was > 80% = 1%  
            % of time cpu util (SW) was > 90% = 0%  
            % of time cpu util (SW) was > 95% = 0%  
-----
```

Set

Utilice el mandato **set** para establecer el período de información.

Sintaxis:

```
set                    tiempo
```

tiempo

Especifica el tiempo corto de ventana.

Valores válidos: De 2 a 30 segundos

Valor por omisión: 5

Parte 3. Comprensión, configuración y funcionamiento de las interfaces

Capítulo 13. Iniciación a las interfaces de red

Los capítulos de este manual describen cómo configurar y supervisar las interfaces de red y los protocolos de capa de enlace soportados por el Direccionador. La finalidad de este capítulo es proporcionarle algunas directrices básicas sobre la configuración y supervisión. Este capítulo también le proporciona los procedimientos básicos y la información necesaria para supervisar las interfaces mediante el mandato **interface** de GWCON. Este capítulo incluye las secciones siguientes:

- “Antes de continuar”
- “Interfaces de red y el mandato interface de GWCON”
- “Acceso a los procesos de configuración y de consola de interfaces de red”
- “Acceso a los procesos de configuración y de consola de protocolos de capa de enlace” en la página 220
- “Definición de interfaces de repuesto” en la página 220

Antes de continuar

Antes de continuar, asegúrese de que está familiarizado con los procedimientos necesarios para acceder a los procesos de configuración de interfaces de red.

Para obtener más información sobre estos procedimientos, consulte las secciones que siguen de este capítulo.

Interfaces de red y el mandato interface de GWCON

Cuando configure interfaces de red, puede que sea necesario visualizar determinada información acerca de interfaces específicas. Aunque algunas interfaces tienen sus propios procesos de consola para la supervisión, el direccionador visualiza las estadísticas para *todas* las interfaces de red instaladas cuando se utiliza el mandato **interface** desde el entorno GWCON. (Consulte la sección “Interface” en la página 126.)

Acceso a los procesos de configuración y de consola de interfaces de red

Las referencias siguientes contienen información previa y ejemplos de cómo acceder a los indicadores de configuración y de consola para las interfaces.

Consulte las secciones “Adición de dispositivos” en la página 16, “Acceso al proceso de configuración de interfaces de red” en la página 16 y “Acceso al proceso de consola de interfaz de red” en la página 20 para obtener la información completa sobre el acceso a los procesos de configuración y de consola de las interfaces. El acceso a estos procesos le permite cambiar y supervisar los parámetros configurables de software para las interfaces de red que se utilizan en el direccionador.

Acceso a los procesos de configuración y de consola de protocolos de capa de enlace

Consulte la sección “Capítulo 1. Introducción” en la página 3 para obtener información completa sobre el acceso a los procesos de configuración y de consola de los protocolos. El acceso a estos procesos le permite cambiar y supervisar los parámetros configurables para los protocolos de capa de enlace soportados por el direccionador.

Definición de interfaces de repuesto

Pueden haber ocasiones en que necesite definir interfaces en el dispositivo que no existen actualmente. Puede realizar esta **reconfiguración dinámica** de un dispositivo definiendo interfaces de repuesto al configurar el dispositivo y, después, utilizando el proceso de consola para activar las interfaces cuando están presentes. Consulte las secciones “Configuración de interfaces de repuesto” en la página 71 y “Activate” en la página 118 para ver los detalles.

Capítulo 14. Configuración de interfaces de Red en Anillo IEEE 802.5

Este capítulo describe los mandatos de configuración y operativos de las interfaces de Red en Anillo. Incluye las secciones siguientes:

- “Acceso al proceso de configuración de interfaces de Red en Anillo”
- “Mandatos de configuración de Red en Anillo”
- “Acceso al proceso de supervisión de interfaces” en la página 224
- “Mandatos de supervisión de interfaces de Red en Anillo” en la página 225
- “Interfaces de Red en Anillo y mandato interface de GWCON” en la página 226
- “Soporte para la reconfiguración dinámica de Red en Anillo” en la página 229

Acceso al proceso de configuración de interfaces de Red en Anillo

Para visualizar el indicador `TKR config>`, entre el mandato `network` seguido por el número de la interfaz de Red en Anillo. Por ejemplo:

```
Config>network 0
Token-Ring interface configuration
TKR Config>
```

Utilice el mandato **list devices** en el indicador `Config>` para visualizar una lista de números de las interfaces configuradas en el direccionador.

Nota: Siempre que cambie un parámetro, debe reiniciar el direccionador para que los cambios surtan efecto.

Mandatos de configuración de Red en Anillo

Esta sección describe los mandatos de configuración de Red en Anillo. Entre los mandatos en el indicador `TKR config>`. La Tabla 24 lista los mandatos de configuración de Red en Anillo.

Tabla 24. Resumen de los mandatos de configuración de Red en Anillo

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página 10.
List	Visualiza la configuración de la interfaz de Red en Anillo seleccionada.
LLC	Accede al entorno y los submandatos de configuración LLC.
Media	Establece el tipo de soporte como blindado o no blindado.
Packet-size	Cambia los valores por omisión de tamaño de paquete para todas las Redes en Anillo.
Set	Establece el temporizador de antigüedad para la antememoria RIF y la dirección física (MAC). También establece las modalidades operativas de dúplex o semi-dúplex.
Source-routing	Habilita o inhabilita el direccionamiento de origen en la interfaz.
Speed	Establece la velocidad de la interfaz en Mbps.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página 11.

List

Utilice el mandato **list** para visualizar la configuración actual para la interfaz de Red en Anillo.

Configuración de interfaces de Red en Anillo

Nota: Si la dirección MAC es 0, se utiliza la dirección de la estación por omisión.

Sintaxis:

list

-

Ejemplo:

list

Token-Ring configuration:

```
Packet size (INFO field): 2052
Speed:                    16 Mb/sec
Media:                    Shielded

RIF Aging Timer:         120
Source Routing:          Enabled
MAC Address:              000000000000
```

Packet size

Tamaño del paquete de Red en Anillo.

Speed Velocidad de la red.

Media Tipo de soporte que la red utiliza, blindado o no blindado.

RIF Aging Timer

Período de tiempo que el direccionador conserva la información contenida en el campo de información de direccionamiento (RIF).

Source Routing

Estado de la característica de direccionamiento en origen, habilitada o inhabilitada.

MAC Address

Dirección MAC configurada que se ha establecido con el mandato **set physical-address**. Si sólo se visualizan ceros, la dirección MAC es la dirección por omisión.

LLC

Utilice el mandato **LLC** para acceder al entorno de configuración LLC. Consulte la sección "Mandatos de configuración LLC" en la página 251 para ver una explicación de cada uno de estos mandatos.

Sintaxis:

llc

Nota: Si APPN no se incluye en la carga de software del direccionador, recibirá el mensaje siguiente si intenta utilizar este mandato:

```
LLC configuration is not available for this network.
```

El entorno de configuración LLC sólo está disponible si se incluye APPN en la carga de software.

Media

Utilice el mandato **media** para cambiar el tipo de soporte de red. El tipo de soporte por omisión es el cable STP. Los valores de tipo de soporte válidos son blindado o no blindado. Entre el mandato media seguido del *tipo-soporte*.

Sintaxis:

media

tipo-soporte

Ejemplo:

`media unshielded`

Packet-Size

Utilice el mandato **packet-size** para cambiar el tamaño máximo de paquete para todas las Redes en Anillo. Entre el mandato **packet-size** seguido del número de bytes deseado.

Sintaxis:

packet-size *bytes*

Tabla 25. Tamaños de paquete válidos de Red en Anillo 4/16

Velocidad de datos de red	Valores (número de bytes)
4 Mbps	De 516 a 4498 Nota: Si se define un valor superior a 4498 para un TR de 4 Mb, el software lo establecerá en 4498. Si el usuario no especifica ningún valor, el valor por omisión es 2052.
16 Mbps	De 516 a 18144 Nota: Si no especifica ningún valor, el valor por omisión es 2052.

Nota: Si se aumentan los tamaños de paquetes, también aumentarán los requisitos de memoria de almacenamiento intermedio.

Set

Utilice el mandato **set** para establecer el temporizador del campo de información de direccionamiento (RIF) y la dirección física (MAC).

Sintaxis:

set *physical-address*
rif-timer

physical-address

Indica si desea definir una dirección administrada localmente para la dirección de subcapa MAC de la interfaz de Red en Anillo o utilizar la dirección de estación de fábrica por omisión (indicada por ceros). La dirección de subcapa MAC es la dirección que la interfaz de Red en Anillo utiliza para recibir y transmitir tramas.

Nota: Si se pulsa **Intro** el valor se deja igual. Si se entra **0** y se pulsa **Intro**, el direccionador utilizará la dirección de estación de fábrica. El valor por omisión es utilizar la dirección de estación de fábrica.

Valores válidos: Cualquier dirección hexadecimal de 12 dígitos.

Valor por omisión: dirección incorporada (indicada por ceros).

Ejemplo:

```
set physical-address
MAC address in 00:00:00:00:00:00 form []?
```

rif-timer

Establece la cantidad máxima de tiempo (en segundos) que se conserva la información de RIF antes que se renueve. El valor por omisión es 120.

Configuración de interfaces de Red en Anillo

Ejemplo:

```
set rif-timer  
RIF aging timer value [120]? 120
```

Source-routing

Utilice el mandato **source-routing** para habilitar o inhabilitar el direccionamiento de origen de la estación final. El direccionamiento de origen es el proceso por el cual las estaciones finales determinan la ruta de origen que se ha de utilizar para cruzar puentes de direccionamiento de origen. El direccionamiento de origen permite que los protocolos IP, IPX y AppleTalk Phase 2 lleguen a los nodos del otro lado del puente de direccionamiento de origen.

Este conmutador es completamente independiente de si esta interfaz proporciona el direccionamiento de origen mediante el reenviador SRT. El valor por omisión es habilitado.

Algunas estaciones no pueden recibir correctamente tramas que contienen un RIF de direccionamiento de origen. Esto es especialmente común entre controladores NetWare. La inhabilitación del direccionamiento de origen en esta situación le permitirá comunicarse con estas estaciones.

Sólo debe habilitarse el direccionamiento de origen si hay puentes de direccionamiento de origen en este anillo a través de los cuales desea puentear los paquetes IP, IPX y AppleTalk Phase 2. También debe habilitarse el direccionamiento de origen para que se puedan devolver los mensajes de respuesta de prueba LLC.

Sintaxis:

```
source-routing          enable  
                          disable
```

Speed

Utilice el mandato **speed** para cambiar la velocidad de los datos. La velocidad por omisión es 4 Mbps. Entre el mandato **speed** seguido del valor de velocidad (en Mbps).

Sintaxis:

```
speed                    valor-velocidad
```

valor-velocidad

La velocidad a la que establece la interfaz de Red en Anillo.

Valores válidos: 4 ó 16 Mbps

Valor por omisión: 4 Mbps

Acceso al proceso de supervisión de interfaces

Para visualizar el indicador de supervisión de Red en Anillo (TKR>), entre el mandato **network** seguido por el número de la interfaz de Red en Anillo. Por ejemplo:

```
+network 0  
TKR>
```

Utilice el mandato **list devices** en el indicador Config> para visualizar una lista de números de las interfaces configuradas en el direccionador.

Configuración de interfaces de Red en Anillo

Siga el procedimiento descrito en la sección “Acceso al proceso de configuración de interfaces de red” en la página 16 para acceder al proceso de supervisión de interfaces para la interfaz descrita en este capítulo. Una vez haya accedido al proceso de supervisión de interfaces deseado, puede empezar a entrar los mandatos de supervisión.

Mandatos de supervisión de interfaces de Red en Anillo

Esta sección resume los mandatos de supervisión de Red en Anillo. Entre los mandatos en el indicador de supervisión TKR>.La Tabla 26 lista los mandatos de supervisión.

Tabla 26. Resumen de los mandatos de supervisión de Red en Anillo

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página 10.
Dump	Visualiza un vuelco de la antememoria RIF.
LLC	Visualiza el indicador de supervisión LLC.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página 11.

Dump

Cuando se habilita el direccionamiento de origen en el proceso `tkr config>`, puede utilizar el mandato **dump** para pedir un vuelco del contenido de la antememoria RIF.

Sintaxis:

dump

Ejemplo:

```
dump
MAC address   State   Usage   RIF
0000C90B1A57 ON_RING Yes      0220
```

MAC address

Visualiza la dirección MAC de la interfaz de Red en Anillo.

State Visualiza uno de los estados de interfaz:

On_ring - indica que se ha encontrado un RIF para un nodo del anillo.

Have_route - indica que se ha encontrado un RIF para un nodo de un anillo remoto.

No_route - se visualiza durante un breve período de tiempo mientras se envía una trama exploradora y el direccionador espera un retorno.

Discovering - indica que el direccionador ha enviado una trama exploradora para volver a descubrir el RIF.

St_route - indica que se ha obtenido una ruta de un explorador de árbol de expansión.

Usage Indica que se ha utilizado un RIF en un paquete. El número es arbitrario y no tiene ningún significado funcional.

RIF Visualiza un código que indica el RIF en hexadecimal.

Configuración de interfaces de Red en Anillo

Nota: El RIF sólo se visualiza si está habilitado el Puenteado de ruta de origen en la interfaz de Red en Anillo.

- Pueden visualizarse los datos del RIF de NetBIOS utilizando la secuencia de mandatos siguiente: **talk 5, protocol ASRT, name-caching, list cache rifs.**
- Pueden visualizarse los datos del RIF de Conmutación de enlace de datos utilizando la secuencia de mandatos siguiente: **talk 5, protocol dlsw, list llc2 session all.**

LLC

Utilice el mandato **LLC** para acceder al indicador de supervisión LLC. Los mandatos LLC se entran en este nuevo indicador. Consulte la sección “Mandatos de supervisión LLC” en la página 255 para ver una explicación de cada uno de estos mandatos.

Sintaxis:

llc

Interfaces de Red en Anillo y mandato interface de GWCON

Aunque las interfaces de Red en Anillo tienen sus propios procesos para la supervisión, el direccionador también visualiza estadísticas completas para las interfaces de red instaladas, cuando se utiliza el mandato **interface** desde el entorno GWCON.

Estadísticas visualizadas para las interfaces de Red en Anillo 802.5

Las estadísticas siguientes se visualizan cuando se entra el mandato **interface <númerored>** para una interfaz de Red en Anillo desde el entorno GWCON.

Nt	Nt'	Interface	Slot-Port	Self-Test Passed	Self-Test Failed	Maintenance Failed
0	0	TKR/0	Slot: 1 Port: 1	1	0	0

Token-Ring/802.5 MAC/data-link on Token-Ring interface

Physical address	08005AFE0106		
Microcode Level	ww19cg		
Network speed	16 Mbps		
Max packet size (INFO)	2052		
Handler state	Ring open		
Last Reported Ring status	SERR CO		
# times Signal lost	0	# times Beacons	0
Hard errors	0	Loss wire faults	0
Auto-removal errors	0	Removes received	0
Ring recovery actions	0		
Line errors	0	Burst errors	0
ARI/FCI errors	0	Inputs dropped	0
Frame copy errors	0	Token errors	0
Lost frames	0		
Input overflows	0	Driver output errors	0

La siguiente sección describe las estadísticas generales de interfaces:

Nt Número de interfaz global

Nt' Sólo se aplica a circuitos de marcación

Interface

El nombre de interfaz y el número de esta interfaz dentro de las interfaces de tipo “intrfc”

Utilización del mandato interface de GWCON

Port Número de puerto

Slot Número de ranura

Self-Test: Pass

Número de veces que la autoprueba ha sido satisfactoria

Self-Test: Fail

Número de veces que la autoprueba ha fallado

Maint: Fail

Número de anomalías de mantenimiento

La siguiente sección describe las estadísticas visualizadas que son específicas de las interfaces de Red en Anillo:

Physical address

Especifica la dirección física de la interfaz de Red en Anillo.

Network speed

Especifica la velocidad de la Red en Anillo que se conecta a la interfaz. El contador de velocidad de red visualiza el número de paquetes que la interfaz puede pasar por segundo.

Max packet size (info)

Visualiza el tamaño máximo de paquete configurado para esa interfaz. El contador de tamaño máximo de paquete visualiza la longitud máxima, en bytes, de un paquete que la interfaz transmite o recibe. Este contador se define por el usuario.

Handler state

Visualiza el estado actual del manejador de la Red en Anillo. El contador del estado del manejador visualiza el estado del manejador después de que se ejecute la autoprueba.

Last ReportedRing status

El último estado de anillo de la interfaz de Red en Anillo.

SIGL SIGNAL_LOSS La interfaz ha detectado una pérdida de señal en el anillo.

HERR HARD_ERROR La interfaz está actualmente transmitiendo o recibiendo tramas de baliza en el anillo.

SERR SOFT_ERROR La interfaz ha transmitido una trama MAC de informe de error.

BEAC TRANSMIT_BEACON La interfaz está transmitiendo tramas de baliza al anillo o desde el mismo.

LWF LOBE_WIRE_FAULT La interfaz ha detectado un circuito abierto o corto en el cable entre la interfaz y el concentrador del cableado. La interfaz se cierra y está en el estado siguiente a la inicialización.

ARMV AUTO_REMOVAL_ERROR La interfaz ha fallado la prueba de reinicio de lóbulo, que ha sido el resultado del proceso de eliminación automática de baliza y se ha eliminado a sí misma del anillo. La interfaz se ha cerrado y está en el estado siguiente a la inicialización.

RMVD REMOVED_RECEIVED La interfaz ha recibido una petición de trama MAC de eliminación de estación de anillo y se ha eliminado a sí misma del anillo. La interfaz se cierra y está en el estado siguiente a la inicialización.

Utilización del mandato interface de GWCON

- CO** COUNTER_OVERFLOW Uno de los siguientes contadores de errores ha aumentado de 254 a 255: Línea, ARI/FCI, Copia de tramas, Tramas perdidas, Ráfaga, Anomalías de cable de lóbulos, Eliminaciones recibidas. Esta pantalla muestra estos contadores de error.
- SSTA** SINGLE_STATION La interfaz ha detectado que es la única estación del anillo.
- RR** RING_RECOVERY La interfaz observa tramas MAC de reclamación de señal en el anillo. La interfaz puede estar transmitiendo tramas de reclamación de señal. Este estado permanece hasta que la interfaz transmite una trama de depuración del anillo.

of times signal lost

Especifica el número total de veces que el direccionador no ha podido transmitir un paquete debido a una pérdida de señal.

Hard errors

Visualiza el número de veces que la interfaz transmite o recibe tramas de baliza de la red.

Auto-removal errors

Visualiza el número de veces que la interfaz, debido a un proceso de autoeliminación de baliza, no puede pasar la prueba de reinicio de lóbulos y se elimina a sí misma de la red.

Ring recovery actions

Visualiza el número de veces que la interfaz detecta tramas de control de acceso al soporte (MAC) de reclamación de señal en la red.

Line errors

El contador de errores de línea se incrementa cuando se repite o copia una trama y el Indicador de error detectado (EDI) es cero para la trama de entrada:

También debe existir una de las condiciones siguientes:

- Existe una señal con una violación de código.
- Una trama contiene una violación de código entre el delimitador inicial y final.
- Se produce un error de Secuencia de comprobación de tramas (FCS).

ARI/FCI errors

El contador de errores ARI/FCI (Indicador de dirección reconocida/Indicador de trama copiada) se incrementa si la interfaz recibe una de las siguientes:

Una trama MAC Monitor activo presente (AMP) con los bits ARI/FCI igual a cero y una trama MAC de Monitor en espera presente (SMP) con los bits ARI/FCI igual a cero.

Más de una trama MAC SMP con los bits ARI/FCI igual a cero, sin ninguna intervención de trama MAC AMP.

Este error indica que el direccionador contiguo en sentido inverso ha copiado la trama pero no puede establecer los bits ARI/FCI.

Frame copy errors

Visualiza el número de veces que la interfaz en modalidad de recepción/repetición reconoce una trama dirigida a su dirección específica pero encuentra que los bits del indicador de dirección reconocida (ARI) no son igual a cero. Este error indica una posible llegada a la línea o una dirección duplicada.

Lost frames

Visualiza el número de veces que la interfaz está en modalidad de transmisión (stripping) y no puede recibir el final de una trama transmitida.

Input overflows

Especifica el número de tramas que se han recibido que eran superiores al tamaño de almacenamiento intermedio de entrada. Las tramas que son demasiado grandes para caber en un sólo almacenamiento intermedio de entrada se eliminan.

times beaconing

Visualiza el número de veces que la interfaz transmite una trama de baliza a la red.

Lobe wire faults

Visualiza el número de veces que la red detecta un circuito abierto o corto en el cable entre la interfaz y el concentrador del cableado.

Removes received

Visualiza el número de veces que la interfaz recibe una petición de trama MAC de eliminación de estación de anillo y se elimina a sí misma de la red.

Burst errors

Visualiza el número de veces que la interfaz detecta la ausencia de transiciones durante cinco medios bits entre el delimitador de inicio (SDEL) y el delimitador de fin (EDEL) o entre el EDEL y el SDEL.

Inputs dropped

Visualiza el número de veces que una interfaz en modalidad de repetición reconoce una trama dirigida a ella pero no tiene espacio de almacenamiento intermedio disponible para copiar la trama.

Token errors

El contador de errores de señal se incrementa cuando el monitor activo detecta un protocolo de señal con cualquiera de los errores siguientes:

El bit MONITOR_COUNT de la señal con prioridad distinta de cero es igual a uno.

El bit MONITOR_COUNT de una trama es igual a uno. No se recibe ninguna señal ni trama en una ventana de 10 ms.

La secuencia de delimitador/señal inicial contiene una violación de código en un área en que las violaciones de código no deben existir.

Soporte para la reconfiguración dinámica de Red en Anillo

Esta sección describe la reconfiguración dinámica (DR) en la medida en que afecta a los mandatos Talk 6 y Talk 5.

Delete Interface de CONFIG (Talk 6)

La Red en Anillo soporta el mandato **delete interface** de CONFIG (Talk 6) con la consideración siguiente:

Cuando se elimina la interfaz, se suprime el registro de direccionamiento de origen y se vuelven a numerar los registros de números mayores.

Activate Interface de GWCON (Talk 5)

La Red en Anillo soporta el mandato **activate interface** de GWCON (Talk 5) sin ninguna restricción.

Utilización del mandato **interface** de GWCON

El mandato **activate interface** de GWCON (Talk 5) soporta todos los mandatos específicos de interfaz de Red en Anillo.

Reset Interface de GWCON (Talk 5)

La Red en Anillo soporta el mandato **reset interface** de GWCON (Talk 5) con la consideración siguiente:

Si se ha establecido el tamaño máximo de paquete en un valor superior al tamaño para los datos del usuario, debe reentrancarse el 2216.

El mandato **reset interface** de GWCON (Talk 5) soporta todos los mandatos específicos de interfaz de Red en Anillo.

Capítulo 15. Configuración y supervisión de la Red en Anillo Rápida

La Red en Anillo Rápida FasTR utiliza los adaptadores ATM existentes del IBM 2216 como adaptadores de la red en anillo rápida. Soporta el direccionamiento IP, DLSw, APPN y SRB (Puentado de ruta de origen).

Este capítulo describe la configuración de la red FasTR y los mandatos operativos para FasTR. Incluye las secciones siguientes:

- “Acceso al proceso de configuración de interfaces FasTR”
- “Mandatos de configuración FasTR”
- “Acceso al proceso de supervisión de interfaces” en la página 234
- “Mandatos de supervisión de la interfaz FasTR” en la página 234
- “Interfaces FasTR y mandato interface de GWCON” en la página 235

Acceso al proceso de configuración de interfaces FasTR

Para visualizar el indicador FasTR `config>`, entre el mandato `network` seguido del número de interfaz de la interfaz FasTR. Por ejemplo:

```
Config>network 0
Fast Token-Ring interface configuration
FasTR Config>
```

Utilice el mandato **list devices** en el indicador `Config>` para visualizar una lista de números de interfaces configuradas en el direccionador.

Nota: Siempre que cambie un parámetro, debe reiniciar el direccionador para que los cambios surtan efecto.

Mandatos de configuración FasTR

Esta sección describe los mandatos de configuración FasTR. Entre los mandatos en el indicador FasTR `config>`. La Tabla 27 lista los mandatos de configuración FasTR.

Tabla 27. Resumen de los mandatos de configuración FasTR

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página 10.
List	Visualiza la configuración de la interfaz FasTR seleccionada.
LLC	Accede al entorno y a los submandatos de configuración LLC.
Media	Toma fibra por omisión. No se permite ninguna entrada.
Packet-size	Establece el tamaño máximo de paquete para las redes FasTR.
Set	Establece el temporizador de antigüedad para la antememoria RIF y la dirección física (MAC).
Source-routing	Habilita o inhabilita el direccionamiento de origen en la interfaz.
Speed	Toma por omisión 155 Mbps. No se permite ninguna entrada.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página 11.

Configuración de la red FasTR

List

Utilice el mandato **list** para visualizar la configuración actual para la interfaz FasTR.

Nota: Si la dirección MAC es 0, se utiliza la dirección de la estación por omisión.

Sintaxis:

```
list
```

Ejemplo:

```
list
```

```
Fast Token-Ring configuration:
    Packet size (INFO field): 2052
    Speed:                    155Mbps
    Media:                    Fiber
    RIF Aging Timer:         120
    Source Routing:          Enabled
    MAC Address:             000000000000
```

Packet size	Tamaño máximo de paquete FasTR.
Speed	Velocidad de la red, 155 Mbps.
Media	Tipo de soporte que la red utiliza, fibra.
RIF Aging Timer	Tiempo que el direccionador conserva la información contenida en el campo de información de direccionamiento (RIF).
Source Routing	Estado de la característica de direccionamiento de origen, habilitado o inhabilitado.
MAC Address	Dirección MAC configurada que se ha establecido con el mandato set physical-address . Si sólo se visualizan ceros, la dirección MAC es la dirección por omisión.

LLC

Utilice el mandato **LLC** para acceder al entorno de configuración LLC. Consulte la sección “Mandatos de configuración LLC” en la página 251 para ver una explicación de cada uno de estos mandatos.

Sintaxis:

```
llc
```

Ejemplo:

```
llc
```

```
LLC config>
```

Nota: Si APPN no se incluye en la carga de software del direccionador, recibirá el mensaje siguiente si intenta utilizar este mandato:

```
LLC configuration is not available for this network.
```

El entorno de configuración LLC sólo está disponible si se incluye APPN en la carga de software.

Media

El tipo de soporte por omisión es la fibra. No se permite ninguna entrada.

Packet-Size

Utilice el mandato **packet-size** para establecer el tamaño máximo de paquete para las redes FasTR. Entre el mandato **packet-size** seguido del número de bytes deseado.

Nota: Si aumenta el tamaño de paquete, también aumentarán los requisitos de memoria de almacenamiento intermedio.

Sintaxis:

`packet-size númerobytes`

Ejemplo:

`packet-size 4399`

Set

Utilice el mandato **set** para establecer el temporizador del campo de información de direccionamiento (RIF) y la dirección física (MAC).

Sintaxis: `set`

`physical-address`

`rif-timer`

physical-address

Indica si desea definir una dirección administrada localmente para la dirección de subcapa MAC de la interfaz FasTR o utilizar la dirección de estación de fábrica por omisión (sólo ceros). La dirección de subcapa MAC es la dirección que la interfaz FasTR utiliza para recibir y transmitir tramas.

Nota: Si se pulsa **Intro** el valor se deja igual. Si se entra **0** y se pulsa **Intro**, el direccionador utilizará la dirección de estación de fábrica. El valor por omisión es utilizar la dirección de estación de fábrica.

Valores válidos: Cualquier dirección hexadecimal de 12 dígitos.

Valor por omisión: dirección incorporada (indicada por ceros).

Ejemplo:

`set physical-address`

MAC address in 00:00:00:00:00:00 form []?

rif-timer

Establece la cantidad máxima de tiempo (en segundos) que se conserva la información de RIF antes de renovarse. El valor por omisión es 120.

Ejemplo:

`set rif-timer`

RIF aging timer value [120]? 120

Source-routing

Utilice el mandato **source-routing** para habilitar o inhabilitar el direccionamiento de origen de la estación final. El direccionamiento de origen es el proceso por el cual las estaciones finales determinan la ruta de origen que se ha de utilizar para cruzar puentes de direccionamiento de origen. El direccionamiento de origen permite que el protocolo IP llegue a nodos del otro lado del puente de direccionamiento de origen.

Este conmutador es completamente independiente de si esta interfaz proporciona el direccionamiento de origen mediante el reenviador SRT. El valor por omisión es habilitado.

Algunas estaciones no pueden recibir correctamente tramas que contienen un RIF de direccionamiento de origen. Esto es especialmente común entre controladores

Configuración de la red FasTR

NetWare. La inhabilitación del direccionamiento de origen en esta situación le permitirá comunicarse con estas estaciones.

El direccionamiento de origen sólo debe habilitarse si hay puentes de direccionamiento de origen en el anillo, a través de los cuales desea puentear paquete IP. También debe habilitarse el direccionamiento de origen para que se puedan devolver los mensajes de respuesta de prueba LLC.

Sintaxis: `source-routing`

`enable`

`disable`

Ejemplo: `source-routing enable`

Speed

La velocidad por omisión es 155 Mbps. No se permite ninguna entrada.

Acceso al proceso de supervisión de interfaces

Para visualizar el indicador de supervisión de red en anillo (TKR>), entre el mandato `network` seguido del número de la interfaz FasTR. Por ejemplo:

```
+network 0
TKR>
```

Utilice el mandato `list devices` en el indicador `Config>` para visualizar una lista de números de interfaces configuradas en el direccionador.

Siga el procedimiento descrito en la sección “Capítulo 13. Iniciación a las interfaces de red” en la página 219 para acceder al proceso de supervisión de interfaces para la interfaz descrita en este capítulo. Una vez haya accedido al proceso de supervisión de interfaces deseado, puede empezar a entrar los mandatos de supervisión.

Mandatos de supervisión de la interfaz FasTR

Esta sección describe los mandatos de supervisión FasTR. Entre los mandatos en el indicador de supervisión TKR>. La Tabla 28 lista los mandatos de supervisión.

Tabla 28. Resumen de los mandatos de supervisión FasTR

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página 10.
Dump	Visualiza un vuelco de la antememoria RIF.
LLC	Visualiza el indicador de supervisión LLC.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página 11.

Dump

Cuando el direccionamiento de origen está habilitado en el proceso FasTR `config>`, puede utilizar el mandato `dump` para pedir un vuelco del contenido de la antememoria RIF.

Sintaxis:

```
dump
```

Ejemplo:

```
dump
```

```
MAC address      State      Usage      RIF
0000C90B1A57    ON_RING    Yes         0220
```

MAC address Visualiza la dirección MAC de la interfaz FasTR.

State Visualiza uno de los estados de interfaz:

On_ring - indica que se ha encontrado un RIF para un nodo del anillo.

Have_route - indica que se ha encontrado un RIF para un nodo de un anillo remoto.

No_route - se visualiza durante un breve período de tiempo mientras se envía una trama exploradora y el direccionador espera un retorno.

Discovering - indica que el direccionador ha enviado una trama exploradora para volver a descubrir el RIF.

St_route - indica que se ha obtenido una ruta de un explorador de árbol de expansión.

Usage Indica que se ha utilizado un RIF en el paquete. El número es arbitrario y no tiene significado funcional.

RIF Visualiza un código que indica el RIF en hexadecimal.

Nota: El RIF sólo se visualiza si el Puenteado de ruta de origen está habilitado en al interfaz FasTR.

- Pueden visualizarse los datos del RIF de NetBIOS utilizando la secuencia de mandatos siguiente: **talk 5, protocol ASRT, name-caching, list cache rifs.**

- Pueden visualizarse los datos del RIF de Conmutación de enlace de datos utilizando la secuencia de mandatos siguiente: **talk 5, protocol dlsw, list llc2 session all.**

LLC

Utilice el mandato **LLC** para acceder al indicador de supervisión LLC. Los mandatos LLC se entran en este nuevo indicador. Consulte la sección "Mandatos de supervisión LLC" en la página 255 para ver una explicación de cada uno de estos mandatos.

Sintaxis:

```
llc
```

Ejemplo:

```
llc
```

```
supervisión de usuario LLC
LLC>
```

Interfaces FasTR y mandato interface de GWCON

Aunque las interfaces FasTR tienen sus propios procesos de supervisión, el direccionador también visualiza estadísticas completas para las interfaces de red instaladas cuando se utiliza el mandato **interface** desde el entorno GWCON.

Estadísticas visualizadas para las interfaces FasTR

Las siguientes estadísticas se visualizan cuando se entra el mandato **interface <número red>** para una interfaz FasTR desde el entorno GWCON.

Utilización del mandato interface de GWCON

```

+i 0
Nt Nt' Interface Slot-Port Self-Test Self-Test Maintenance Failed
0 0 TKR/0 Slot: 1 Port: Passed 1 Failed 1 Failed 0
0

Token-Ring/802.5 MAC/data-link on Fast Token Ring interface

Physical address 000000019100
Network speed 155 Mbps
Max packet size (INFO) 2052
Handler state Ring open

Hdr Thresh: 0 Bad CRC: 0
Bad Length: 0 Max Len Exc.: 0
Rcv Timeout: 0 Fwd Aborts: 0
Nonzero CPI: 0

Cells Rcvd: 0 NUD Rcvd: 0
NUD Bad CRC: 0 Bad HEC: 0

LCD Events:
AAL0 No Buf: 0 AAL5 No Buf: 0
NUD No Buf: 0
Rx No Sysbuf: 0 Tx No Chrmbf: 0

GPDMA Events:
Tx DMA Error: 0 Rx DMA Error: 0
Buf Overflow: 0 Virt Mem Res: 0
Lost Events: 0 Ill. Events: 0
+

```

La siguiente sección describe las estadísticas de interfaz general:

Nt	Número de interfaz global
Nt'	Sólo se aplica a circuitos de marcación
Interface	El nombre de interfaz y el número de esta interfaz dentro de las interfaces de tipo <i>intrfc</i>
Slot-Port	Número de ranura y número de puerto
Self-Test: Pass	Número de veces que la autoprueba ha sido satisfactoria
Self-Test: Fail	Número de veces que la autoprueba ha fallado
Maintenance Failed	Número de anomalías de mantenimiento

La siguiente sección describe las estadísticas visualizadas que son específicas de las interfaces FasTR:

Physical address	Especifica la dirección física de la interfaz FasTR.
Network speed	Especifica la velocidad de la red FasTR que se conecta a la interfaz. El contador de velocidad de red visualiza el número de paquetes que la interfaz puede pasar por segundo.
Max packet size (info)	Visualiza el tamaño máximo de paquete configurado para esa interfaz. El contador de tamaño máximo de paquete visualiza la longitud máxima, en bytes, de un paquete que la interfaz transmite o recibe. Este contador está definido por el usuario.
Handler state	Visualiza el estado actual del manejador de FasTR. El contador del estado del manejador visualiza el estado del manejador después de que se ejecute la autoprueba.
Hdr Thresh	Umbral de cabecera de paquete excedidos.
Bad CRC	Paquetes recibidos con CRC incorrecto.
Bad Length	Paquetes recibidos con longitud incorrecta.
Max Len Exc.	Paquetes recibidos que exceden la longitud máxima.
Rcv Timeout	Tiempos de espera excedido al ensamblar los paquetes recibidos.
Fwd Aborts	Paquetes recibidos terminados con una cancelación anormal de reenvío.
Nonzero CPI	Paquetes recibidos con el campo CPI no establecido en cero.

Utilización del mandato interface de GWCON

Cells Received	Células recibidas (no paquetes).
NUD Rcvd	Campos de datos que no son del usuario recibidos.
NUD Bad CRC	Campos de datos que no son del usuario recibidos con CRC_10 incorrecto.
Bad HEC	Células recibidas con Comprobación de error de cabecera incorrecta.
Sucesos LCD	
AAL0 No Buf	Células AAL0 eliminadas debido a una falta de almacenamientos intermedios de agrupaciones.
AAL5 No Buf	Células AAL5 eliminadas debido a una falta de almacenamientos intermedios de agrupaciones.
NUD No Buf	Datos que no son de usuario eliminados debido a la falta de almacenamientos intermedios de agrupaciones.
Rx No Sysbuf	Paquetes recibidos pero eliminado debido a que no habían almacenamientos intermedios del sistema disponibles.
Tx No Chrmbuf	Paquetes de transmisión eliminados porque no estaba disponible ningún almacenamiento intermedio de adaptador.
GPDMA Events	
Tx DMA Error	DMA de transmisión con errores.
Rx DMA Error	DMA de recepción con errores.
Buf Overflow	Paquetes recibidos que excedían el tamaño real de almacenamiento intermedio.
Virt Mem Res	Sucesos de recurso de Memoria virtual, grabando células en memoria virtual.
Lost Events	Sucesos perdidos debido a que la cola de recepción estaba llena.
Ill. Events	Sucesos no reconocidos.

Utilización del mandato interface de GWCON

Capítulo 16. Utilización de FDDI

Este capítulo describe cómo establecer la información configurable por el software para Fiber Distributed Data Interface (FDDI) en el direccionador.

Este capítulo contiene las secciones siguientes:

- “Visión general de Fiber Distributed Data Interface (FDDI)”

Visión general de Fiber Distributed Data Interface (FDDI)

Fiber Distributed Data Interface (FDDI) se describe por las comisiones ANSI X3T9.5 y ISO 9314 como un anillo de rotación de contador dual que opera a una velocidad definida de 100 Mbps.

En muchos puntos, FDDI es similar a la red en anillo IEEE 802.5, aunque existen diferencias, algunas de las cuales se describen en la sección “Diferencias entre FDDI y Red en Anillo” en la página 240.

Red en anillo de paso de señales

FDDI se define como un protocolo de paso de señales. Cada estación tiene la oportunidad de transmitir datos cuando pasa una señal. Una estación puede decidir cuántas tramas transmitirá utilizando un algoritmo que permite la asignación de “ancho de banda”.

FDDI también permite que una estación transmita muchas tramas sin liberar la señal de manera similar al estándar de red en anillo IEEE 802.5.

Una red en anillo FDDI consta de un conjunto de estaciones/dispositivos conectados como una cadena serie de estaciones/dispositivos y un soporte de transmisión, formando un bucle cerrado físicamente. La información se transmite secuencialmente como una corriente de señales convenientemente codificadas desde una estación/dispositivo activo al siguiente activo.

Generalmente, cada estación/dispositivo vuelve a generar y repite cada señal y puede servir de medio de conexión de una o varias estaciones/dispositivos con la red.

Anillos primarios y secundarios

FDDI define dos anillos:

- El *anillo primario*, que es similar a la vía de acceso del anillo principal de una red en anillo.
- El *anillo secundario*, que es similar a la vía de acceso de anillo de reserva de una red en anillo.

Cada vía de acceso de anillo consta de dos fibras, cada una transmite una señal; una se envía y otra se recibe en un dispositivo. Cada fibra es equivalente a un par de conductores de cobre. El enfoque físico de los términos de fibras ópticas es similar a las vías de acceso de la red en anillo de fibra óptica física.

Conexión de dispositivos

FDDI permite muchas unidades de conexión:

- Estaciones o dispositivos
- Concentradores

Utilización de FDDI

- Puentes

Estas unidades pueden conectarse a redes FDDI de varias maneras, parecidas a las redes en anillo.

Diferencias entre FDDI y Red en Anillo

Las diferencias principales entre las técnicas de FDDI y de red en anillo son:

- Un dispositivo se puede conectar directamente a anillos sin ningún concentrador como, por ejemplo, una unidad de acceso a multiestación (MSAU) de una red en anillo.
- Un dispositivo se puede conectar a uno o a los dos anillos, primario y secundario.

FDDI define dos clases de dispositivos, A y B, para diferenciar los dispositivos que se conectan a un anillo o a ambos anillos, tal como se describe en la siguiente sección.

Clases de dispositivos A y B

FDDI define dos clases de dispositivos:

- Un dispositivo de **Clase A** se conecta a los dos anillos directamente.
Puede ser una estación, llamada una *estación de Clase A* o *Estación de acceso dual (DAS)* o puede ser un Concentrador llamado un *Concentrador de acceso dual (DAC)*
- Un dispositivo de **Clase B** sólo se conecta a uno de los anillos directamente o a través de un concentrador.
Puede ser una estación, llamada una *estación de Clase B* o *Estación de acceso único (SAS)* o puede ser un Concentrador, llamado un *Concentrador de acceso único (SAC)*

Diagrama de red FDDI

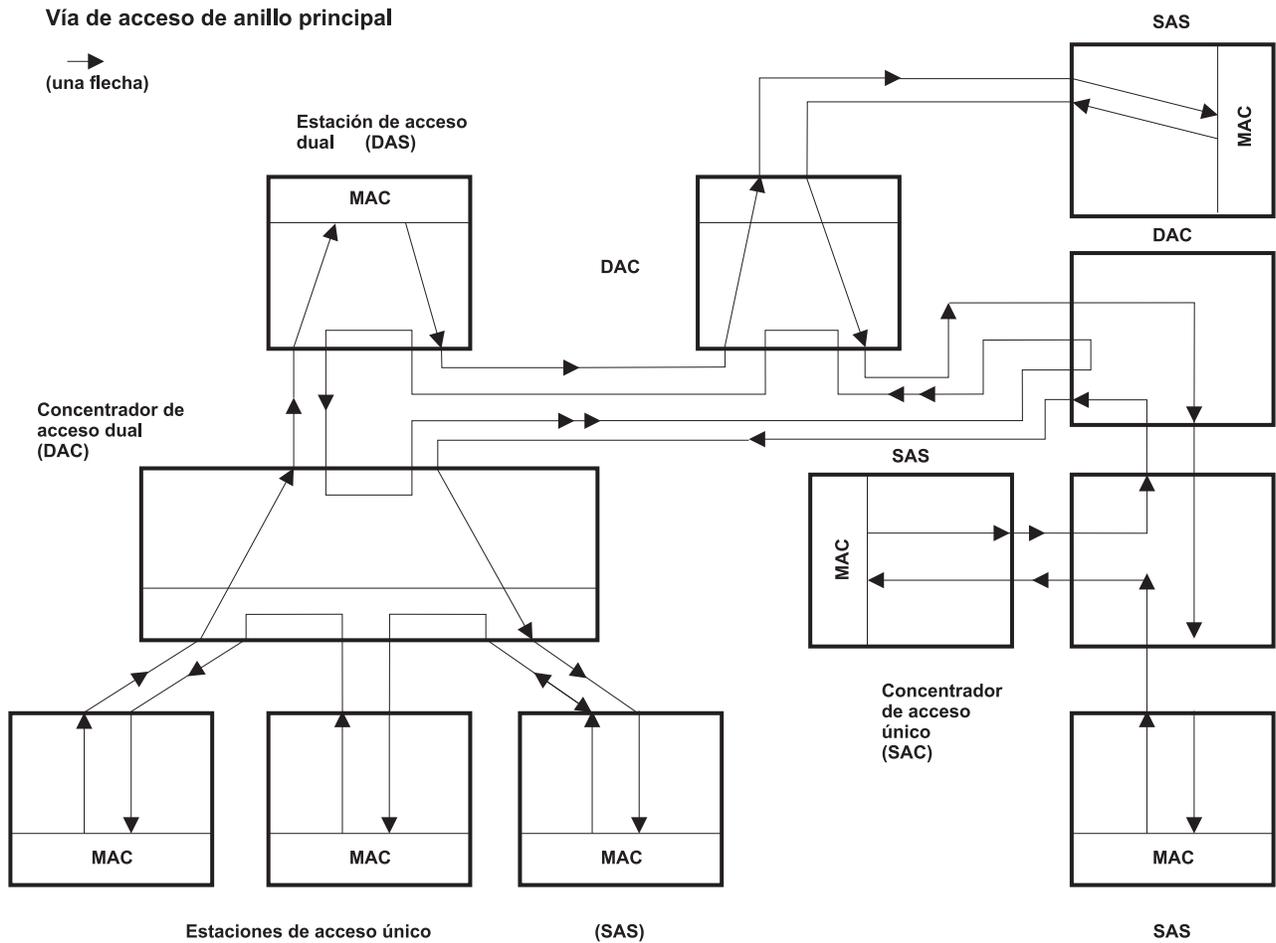


Figura 14. Diagrama de red FDDI. Este diagrama muestra las Estaciones de acceso único (SAS), las Estaciones de acceso dual (DAS), los Concentradores de acceso único (SAC) y los Concentradores de acceso dual (DAC) en una Vía de acceso de anillo principal de una red FDDI.

Capítulo 17. Configuración y supervisión de FDDI

Este capítulo describe los mandatos de configuración y operativos de la interfaz FDDI. Incluye las secciones siguientes:

- “Acceso a los mandatos de configuración FDDI”
- “Mandatos de configuración FDDI”
- “Acceso a los mandatos de supervisión FDDI” en la página 246
- “Mandatos de supervisión FDDI” en la página 246

Acceso a los mandatos de configuración FDDI

Puede acceder a la configuración FDDI desde Talk 6. Para hacerlo, entre el mandato **add device** para añadir una interfaz FDDI a la red y asignarle un número de interfaz y, después, utilice el mandato **network** para acceder a la interfaz FDDI tal como se muestra en el ejemplo siguiente:

```
Config> add device fddi
SK-NET FDDI device in slot 0 port 1 as interface #2
Use "net 2" to configure SK-NET FDDI parameters

Config> network ?
0 :CHARM ATM Adapter
1 :ATM Token Ring LAN Emulation: elan1
2 :SK-NET FDDI

Config> network 2
FDDI Interface Configuration
FDDI Config>
```

Esto le llevará al indicador FDDI Config>.

Cuando haya terminado, entre **Exit** para volver al nivel de indicador anterior.

Mandatos de configuración FDDI

Esta sección describe los mandatos de configuración FDDI, tal como se muestra en la Tabla 29. Entre los mandatos en el indicador FDDI Config>.

Tabla 29. Resumen de los mandatos de configuración FDDI

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página 10.
List	Visualiza la configuración FDDI seleccionada.
LLC	Proporciona acceso al entorno de configuración LLC.
Set	Establece los parámetros FDDI.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página 11.

List

Utilice el mandato **list** para visualizar la configuración actual de FDDI.

Sintaxis:

list

all

all Lista toda la salida para los diversos parámetros que siguen.

Configuración de FDDI

```
FDDI Config [4]>LIST ALL
FDDI configuration:

Locally Admin. Address: 40:00:00:12:34:56
T_Max (in ms): 165 (default)
T_Min (in ms): 5 (default)
Requested Target Rotation Time (in ms): 165 (default)
Valid transmission expiration timer (in us): 2500 (default)
Link Error Rate Alarm Port A: 100-8 (default)
Link Error Rate Cutoff Port A: 100-7 (default)
Link Error Rate Alarm Port B: 100-8 (default)
Link Error Rate Cutoff Port B: 100-7 (default)
PMF password:
User data:
```

LLC

Utilice el mandato **LLC** para acceder al entorno de configuración LLC. Consulte la sección "Mandatos de configuración LLC" en la página 251 para ver una explicación del mandato LLC.

Sintaxis:

llc

Set

Utilice el mandato **set** para configurar FDDI.

Sintaxis:

```
set                ler
                   physical-address
                   pmf
                   tmax
                   tmin
                   freq
                   tvx
                   userdata
```

ler númeropuerto tipo

Establece los valores de alarma e interrupción para el puerto A y el puerto B de la manera siguiente:

ler a alarm

Establece los valores de alarma para el puerto A.

ler a cutoff

Establece los valores de interrupción para el puerto A.

ler b alarm

Establece los valores de alarma para el puerto B.

ler b cutoff

Establece los valores de interrupción para el puerto B.

Valores válidos y valores por omisión

Alarma o interrupción	Valores válidos	Valor por omisión
Alarma	De 4 a 15	8
Interrupción	De 4 a 15	7

physical-address

Indica si desea definir una dirección administrada localmente para la dirección de subcapa MAC de la interfaz FDDI o utilizar la dirección de estación de fábrica por omisión (indicada por sólo ceros). La dirección de subcapa MAC es la dirección que la interfaz FDDI utiliza para recibir y transmitir tramas.

Nota: Si se pulsa **Intro** el valor se deja igual. Si se entra **0** y se pulsa **Intro** hace que el direccionador utilice la dirección de estación de fábrica. El valor por omisión es utilizar la dirección de estación de fábrica.

Valores válidos: Cualquier dirección hexadecimal de 12 dígitos.

Valor por omisión: dirección incorporada (indicada por ceros).

Ejemplo:

```
set physical-address
MAC address in 00:00:00:00:00:00 form []?40:00:00:12:34:56
```

pmf

Establece la contraseña PMF (8 caracteres como máximo).

tmax

Establece el Tiempo máximo de rotación de señal (en milisegundos) que esta estación puede aceptar. Normalmente se hace referencia T_Max en las especificaciones FDDI.

Valores válidos: De 5 a 165 milisegundos

Valor por omisión: 165 milisegundos

tmin

Establece el Tiempo mínimo de rotación de señal (en milisegundos) que esta estación puede aceptar. Si el TTRT negociado es menor que este valor, el adaptador no proporcionará el servicio adecuado a las capas por encima suyo. Normalmente se hace referencia como T_Min en las especificaciones FDDI.

Valores válidos: De 5 a 165 milisegundos

Valor por omisión: 5 milisegundos

treq

Establece el Tiempo de rotación de señal de destino pedido (en milisegundos) que esta estación solicitará durante la inicialización. Normalmente se hace referencia como T_Req en las especificaciones FDDI.

Valores válidos: De 5 a 165 milisegundos

Valor por omisión: 165 milisegundos

tvx

Establece la caducidad del temporizador de transmisión válida (en microsegundos). Este temporizador se restablece cada vez que la estación ve una trama válida o una señal no restringida. Si caduca el temporizador, indica que el tráfico no está circulando adecuadamente en el anillo y, por lo tanto, se inicia un proceso de reclamación. Normalmente se hace referencia como TVX en las especificaciones FDDI.

Valores válidos: De 2500 a 10 000 microsegundos

Valor por omisión: 2500 microsegundos.

userdata

Establece los datos de usuario (32 caracteres como máximo).

Acceso a los mandatos de supervisión FDDI

Puede acceder a la configuración FDDI desde Talk 5 entrando el mandato **network** para acceder a la interfaz FDDI, tal como se muestra en el ejemplo siguiente:

```
network ?
0  :CHARM ATM Adapter
1  :ATM Token Ring LAN Emulation: elan1
2  :SK-NET FDDI

network 2
FDDI Interface
FDDI>
```

Esto le llevará al indicador FDDI>.

Cuando haya terminado, entre **Exit** para volver al nivel de indicador anterior.

Mandatos de supervisión FDDI

Los mandatos de supervisión para FDDI son:

Tabla 30. Resumen de los mandatos de supervisión FDDI

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado "Cómo obtener ayuda" en la página 10.
List	Visualiza la información de adaptador FDDI
LLC	Visualiza el indicador de supervisión LLC.
Srt-stat	Visualiza las estadísticas de puente FDDI.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página 11.

List

Utilice el mandato **list** para visualizar los parámetros de configuración FDDI actuales.

Sintaxis:

list

Ejemplo:

```
FDDI> list
MAC Address: 40:00:00:12:34:56
Bridging Disabled
```

LLC

Utilice el mandato **LLC** para acceder al entorno de configuración LLC. Consulte la sección "Mandatos de configuración LLC" en la página 251 para ver una explicación del mandato LLC.

Sintaxis:

llc

Srt-stat

Utilice el mandato **srt-stat** para visualizar las estadísticas puenteadas asistidas por hardware de esta interfaz.

Sintaxis:**srt-stat****Ejemplo:**

```

srt-stat
Port Supports:                Transparent Bridging Only

Frames received:                806
Bytes received:                 34588
Maximum size of filter table in adapter: 4088
Number of entries in filter table: 0
Number of dynamic entries in filter table: 0

```

Interfaces FDDI y el mandato GWCON

Aunque las interfaces FDDI tienen sus propios procesos de supervisión, el direccionador también visualiza estadísticas completas para las interfaces de red instaladas cuando se utiliza el mandato `interface` desde el entorno GWCON.

Estadísticas visualizadas desde interfaces FDDI

Las estadísticas siguientes se visualizan cuando se entra el mandato `interface númerored` para una interfaz FDDI desde el entorno GWCON.

Nt	Nt'	Interface	Slot-Port	Self-Test Passed	Self-Test Failed	Maintenance Failed
0	0	FDDI/0	Slot: 1 Port: 1	1	0	0

IEEE 802.2/FDDI MAC/data-link on SK-NET FDDI interface

Address: 00:60:94:C4:00:40

UNA: 00:00:5A:02:2D:1E -> DNA: 00:00:5A:02:2D:1E

```

-----
ECM State Machine:          IN
PCM State Machine Port A:  SIGNAL
PCM State Machine Port B:  ACTIVE
CFM State Machine Port A:  ISOLATED
CFM State Machine Port B:  CONCATENATED
CF State Machine:           C_WRAP_B
MAC Current Path:           PRIMARY
RMT State Machine:          RING_OP
-----

```

```

-----
TVX expired ct: 0
Beacon ct:      0
Claim ct:       0
RingOp ct:      1
-----

```

```

-----
PHYA:LEM_Ct: 0 LEM Reject Ct: 0 LCT fails: 40
Alarm: 10^-8 CuTtoff: 10^-7 Estimate: 10^-15
PHYB:LEM_Ct: 0 LEM Reject Ct: 0 LCT fails: 40
Alarm: 10^-8 CuTtoff: 10^-7 Estimate: 10^-15
-----

```

T_Notify 10 sec, SMT frames in:55363 SMT frames out:35317

Frames:211764, Errors:0, Losts:0, Xmts:144058, Copied:171046, Not Copied:0

La siguiente sección describe las estadísticas de interfaz general:

Nt Número de interfaz global

Nt' Sólo se aplica a circuitos de marcación

interface

El nombre de interfaz y el número de esta interfaz dentro de las interfaces de tipo *intrfc*.

Port Número de puerto

Slot Número de ranura

Self-Test Passed

Número de veces que la autoprueba ha sido satisfactoria.

Supervisión FDDI

Self-Test Failed

Número de veces que la autoprueba ha fallado.

Maintenance Failed

Número de anomalías de mantenimiento.

La siguiente sección describe las estadísticas visualizadas que son específicas de las interfaces FDDI:

Address

Especifica la dirección física de la interfaz FDDI.

UNA Especifica la dirección física del direccionador contiguo en sentido inverso.

DNA Especifica la dirección física del direccionador contiguo en sentido directo.

ECM State Machine

La Gestión de coordinación de la entidad controla la gestión de la interfaz de soporte, incluyendo todos los puertos del nodo. También controla el desvío óptico.

OUT
IN
TRACE
LEAVE
PATH-TEST
INSERT
CHECK
DEINSERT

PCM State Machine

La Gestión de conexión física controla la gestión de la conexión física entre un puerto que se está gestionando y otro puerto del nodo adyacente.

OFF
BREAK
TRACE
CONNECT
NEXT
SIGNAL
JOIN
VERIFY
ACTIVE
MAINT

CFM State Machine

La Gestión de la configuración gestiona la configuración de los MAC y los puertos de un nodo.

ISOLATED
LOCAL
SECONDARY
PRIMARY
CONCATENATED
THRU

CF State Machine

Configuración de conexión.

ISOLATED
LOCAL_A
LOCAL_B
LOCAL_AB
LOCAL_S
WRAP_A
WRAP_B
WRAP_AB
WRAP_S
C_WRAP_A
C_WRAP_B
C_WRAP_S
THRU

MAC Current Path

Vía de acceso actual en el que este MAC está insertado.

ISOLATED
LOCAL
SECONDARY
PRIMARY

RMT State Machine.

La Gestión de anillo controla la sincronización de las tramas de gestión MAC.

ISOLATED
NON_OP
RING_OP
DETECT_BEACON
NON_OP_DUP
RING_OP_DUP
DIRECTED
RM-TRACE
DETECT_CLAIM
DETECT_IDLE

TVX expired ct

Número de veces que el TVX ha caducado.

Beacon ct

Número de veces que se ha entrado en estado de baliza.

Claim ct

Número de veces que se ha entrado en estado de reclamación.

RingOp ct

Número de veces que el anillo ha entrado en estado operativo.

LEM_Ct

Cuenta de errores de supervisor de errores de enlace.

LCT fails

Cuenta de veces consecutivas que ha fallado la prueba de confianza de enlace.

Alarm Estimación en la que una conexión de enlace generará una alarma.

Cutoff Estimación en la que una conexión de enlace se interrumpirá.

Estimate

Promedio a largo plazo de velocidad de errores de enlace.

Frames

Número de tramas recibidas.

Errors Número de tramas erróneas detectadas.

Losts Número de errores de formato durante la recepción.

Xmts Número de tramas transmitidas.

Copied

Número de tramas copiadas.

Not Copied

Número de tramas no copiadas.

T_Notify

Temporizador de notificación de direccionador contiguo.

SMT frames in

Número de tramas SMT recibidas.

SMT frames out.

Número de tramas SMT enviadas.

Supervisión FDDI

Capítulo 18. Configuración y supervisión de interfaces LLC

Este capítulo describe cómo configurar interfaces LLC específicas del direccionador utilizando los mandatos de interfaz o el mandato interface de GWCON.

Se puede decir que el Nivel de enlace lógico es un “subprotocolo”. No se accede directamente desde el entorno Talk 6 (configuración) ni desde el entorno Talk 5 (supervisión). En su lugar, se accede desde los protocolos de Red en Anillo, Point-to-Point (PPP) o Frame Relay entrando un mandato **LLC**.

Este capítulo incluye las secciones siguientes:

- “Acceso al proceso de configuración de interfaces”
- “Acceso al proceso de supervisión de interfaces” en la página 254
- “Mandatos de supervisión LLC” en la página 255
- “Mandatos de configuración LLC”

Acceso al proceso de configuración de interfaces

Acceda a los mandatos de configuración para el protocolo que desee configurar a través de LLC:

- Red en Anillo, tal como se describe en la sección “Capítulo 14. Configuración de interfaces de Red en Anillo IEEE 802.5” en la página 221
- Point-to-Point, tal como se describe en la sección “Capítulo 43. Utilización de interfaces de Point-to-Point Protocol” en la página 621
- Frame Relay, tal como se describe en la sección “Capítulo 41. Utilización de interfaces Frame Relay” en la página 531
- FDDI, tal como se describe en la sección “Capítulo 16. Utilización de FDDI” en la página 239

Cada uno de estos niveles de indicador tiene un mandato LLC. Entre **LLC** para acceder a los mandatos de configuración LLC y realizar la configuración LLC. Cuando haya terminado, entre **Exit** para volver al nivel de indicador para el protocolo que esté configurando.

Mandatos de configuración LLC

La configuración de LLC es necesario cuando se han de pasar paquetes a través de una red SNA. Para entrar estos mandatos, primero debe entrar en el entorno de configuración LLC (consulte la sección “Acceso al proceso de configuración de interfaces de Red en Anillo” en la página 221).

Esta sección resume y explica todos los mandatos de configuración LLC. Estos mandatos, que aparecen en la Tabla 31, le permiten configurar LLC cuando necesita pasar paquetes a través de una red SNA.

Tabla 31. Resumen de los mandatos de configuración LLC

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página 10.
List	Visualiza la configuración LLC seleccionada.
Set	Establece los temporizadores asociados con LLC y el tamaño de las ventanas de transmisión y recepción.

Configuración de LLC

Tabla 31. Resumen de los mandatos de configuración LLC (continuación)

Mandato	Función
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página 11.

List

Utilice el mandato **list** para visualizar la configuración actual para LLC.

Sintaxis:

list

Ejemplo:

```
list
Reply Timer (T1):          1 seconds
Receive ACK Timer (T2):    100 milliseconds
Inactivity Timer (Ti):     30 seconds
Max Retry value (N2):      8
Rcvd I-frames before ACK (N3): 1
Transmit Window (Tw):      2
Receive Window (Rw):       2
Acks needed to increment Ww (Nw): 1
```

Reply Timer (T1)

Este temporizador caduca cuando LLC no puede recibir un reconocimiento o una respuesta necesarios de otra estación LLC.

Receive ACK Timer (T2)

Este temporizador se utiliza para retrasar el envío de un reconocimiento para una trama recibida en formato I.

Inactivity Timer (Ti)

Este temporizador caduca cuando LLC no recibe ninguna trama durante un período de tiempo especificado. Cuando este temporizador caduca, LLC transmite un RR hasta que otro LLC responde o se excede la cuenta de reintentos N2. El valor por omisión es de 30 segundos.

Max Retry value (N2)

El número máximo de reintentos para el protocolo LLC. El valor por omisión es 8.

Rcvd I-frames before ACK (N3)

Este valor se utiliza con el temporizador T2 para reducir el tráfico de reconocimientos para las tramas I recibidas. Este contador establece un valor especificado y se reduce cada vez que se recibe una trama I. Cuando este contador llega a 0 o caduca el temporizador T2, se envía un reconocimiento. El valor por omisión es 1.

Receive Window (Rw)

Indica el número máximo de tramas I numeradas secuencialmente no reconocidas que un LLC puede recibir desde un sistema principal remoto.

Transmit Window (Tw)

Indica el número máximo de tramas I que pueden enviarse antes de recibir un RR.

Acks needed to increment Ww (Nw)

Este campo se establece en el valor por omisión 1.

Set

Utilice el mandato **set** para configurar el LLC.

Atención: El cambio de los valores por omisión de los parámetros LLC puede afectar a la forma en que funciona el protocolo LLC.

Sintaxis:

set n2-max-retry *cuenta*
n3-frames-rcvd-before-ack *cuenta*
nw-acks-to-inc-window *cuenta*
rw-receive-window *cuenta*
t1-reply-timer *segundos*
t2-receive-ack-timer *segundos*
ti-inactivity-timer *segundos*
tw-transmit-window *cuenta*

n2-max-retry

El número máximo de reintentos del protocolo LLC. Por ejemplo, N2 es el número máximo de veces que el LLC transmite un RR sin recibir un reconocimiento cuando caduca el temporizador de inactividad. El valor por omisión es 8. El mínimo es 1. El máximo es 127.

Ejemplo:

```
set n2-max-retry  
Max Retry value (N2) [8]?
```

n3-frames_rcvd-before-ack

Este valor se utiliza con el temporizador T2 para reducir el tráfico de reconocimientos para las tramas I recibidas. Establezca este contador en un valor especificado. Cada vez que se recibe una trama I, se reduce este valor. Cuando este contador llega a 0 o caduca el temporizador T2, se envía un reconocimiento. El valor por omisión es 1. El mínimo es 1. El máximo es 255.

Ejemplo:

```
set n3-frames_rcvd-before-ack  
Number I-frames received before sending ACK(N3) [1]?
```

rw-receive-window

Indica el número máximo de tramas I numeradas secuencialmente no reconocidas que un LLC puede recibir desde un similar LLC remoto. Este valor debe ser igual o inferior a 127.

Ejemplo:

```
set rw-receive-window  
Receive Window (Rw), 127 Max. [2]?
```

nw-acks-to-inc-ww

Este campo se establece en el valor por omisión 1.

t1-reply-timer

Este temporizador caduca cuando LLC no puede recibir un reconocimiento o una respuesta necesarios de otra estación LLC. Cuando este temporizador caduca, se envía un RR con el bit de sondeo activado y se vuelve a iniciar T1. Si el LLC no recibe ninguna respuesta después del número máximo de reintentos configurados (N2), el enlace subyacente se declara no operativo. El valor por omisión es 1. El mínimo es 1. El máximo es 256.

Ejemplo:

Configuración de LLC

```
set t1-reply-timer
Reply Timer (T1) in sec. [1]?
```

t2-receive-ack-timer

Este temporizador se utiliza para retrasar el envío de un reconocimiento para una trama recibida en formato I. Este temporizador se inicia cuando se recibe una trama I. El temporizador se restablece cuando se envía un reconocimiento. Si este temporizador caduca, LLC2 envía un reconocimiento lo antes posible. Establezca este valor de modo que sea inferior al de T1. Esto asegura que el similar LLC2 remoto reciba el reconocimiento retrasado antes de que caduque el temporizador T1. El valor por omisión es 1 (100 ms). El mínimo es 1. El máximo es 2560.

Ejemplo:

```
set t2-receive-ack-timer
Receive Ack timer (T2) in 100 millisec. [1]?
```

Nota: Si se establece este temporizador en 1 (valor por omisión) no se ejecutará (por ejemplo, `n3-frames_rcvd-before-ack =1`).

ti-inactivity-timer

Este temporizador caduca cuando LLC no recibe ninguna trama durante un período de tiempo especificado. Cuando este temporizador caduca, LLC transmite un RR hasta que otro LLC responde o se excede la cuenta de reintentos N2. El valor por omisión es de 30 segundos. El mínimo es 1 segundo. El máximo es 256 segundos.

Ejemplo:

```
set ti-inactivity-timer
Inactivity Timer (Ti) in sec. [30]?
```

tw-transmit-window

Establece el número máximo de tramas I que pueden enviarse antes de recibir un RR. Suponiendo que el otro extremo de la sesión LLC pueda realmente recibir esta cantidad de tramas I consecutivas y que el direccionador tenga suficiente memoria de almacenamiento dinámico para conservar copias de estas tramas hasta que se reciba un reconocimiento, si se incrementa este valor puede incrementarse la productividad. El valor por omisión es 2. El mínimo es 1. El máximo es 127.

Ejemplo:

```
set tw-transmit-window
Transmit Window (Tw), 127 Max. [2]?
```

Acceso al proceso de supervisión de interfaces

Acceda a los mandatos de supervisión para el protocolo que desee supervisar a través de LLC:

- Red en Anillo, tal como se describe en la sección “Capítulo 14. Configuración de interfaces de Red en Anillo IEEE 802.5” en la página 221
- Point-to-Point, tal como se describe en la sección “Capítulo 44. Configuración y supervisión de interfaces Point-to-Point Protocol” en la página 639
- Frame Relay, tal como se describe en la sección “Capítulo 42. Configuración y supervisión de interfaces Frame Relay” en la página 561
- FDDI, tal como se describe en la sección “Capítulo 16. Utilización de FDDI” en la página 239

Cada uno de estos niveles de indicador tiene un mandato LLC. Entre **LLC** para acceder a los mandatos de supervisión LLC para supervisar LLC. Cuando haya terminado, entre **Exit** para volver al nivel de indicador para el protocolo que está supervisando.

Mandatos de supervisión LLC

Esta sección resume y explica todos los mandatos de supervisión LLC. Estos mandatos, que aparecen en la Tabla 32, le permiten supervisar el LLC mientras pasa paquetes a través de una red SNA.

Tabla 32. Resumen de los mandatos de supervisión LLC

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado "Cómo obtener ayuda" en la página 10.
Clear-counters	Borra todos los contadores de estadísticas.
List	Visualiza la información de interfaz, de SAP y de sesión.
Set	Permite que el usuario configure dinámicamente los parámetros LLC que son válidos para la duración de la sesión.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página 11.

Clear-Counters

Utilice el mandato **clear-counters** para borrar todos los contadores de estadísticas LLC.

Sintaxis:

clear-counters

List

Utilice el mandato **list** para visualizar la información de interfaz, de punto de acceso a servicios (SAP) y de sesión.

Sintaxis:

```
list                interface
                    sap . . .
                    session
```

interface

Visualiza todos los SAP abiertos en esta interfaz.

Ejemplo:

```
list interface
SAP      Number of Sessions
F4       1
```

sap número_sap

Visualiza información para el SAP especificado en la interfaz.

Ejemplo:

```
list sap
SAP value in hex (0FE) [1]? F4
```

Supervisión de LLC

```
Interface 0, TKR/0
Reply Timer(T1) 1 sec
Receive ACK Timer (T2) 100 millisec
Inactivity Timer (Ti) 30 sec
MAX Retry Value (N2) 8
MAX I-field Size (N1) 2052
Rcvd I-frames before ACK (N3) 1
Transmit Window Size (Tw) 2
Acks Needed to Inc Ww (Nw) 1

Frame Xmt Rcvd
UI-frames 4 5
TEST-frames 0 1
XID-frames 0 0
I-frames 291 26
RR-frames 81 291
RNR-frames 0 0
REJ-frames 0 0
SABME-frames 1 0
UA-frames 0 1
DISC-frames 0 0
DM-frames 0 0
FRMR-frames 0 0
I-frames discarded by LLC 0
I-frames Refused by LLC user 0

Cumulative number of sessions 1
Number of active sessions 1

Session ID Remote
(int-sap-id) Local MAC Remote MAC SAP State
00F40000 00:00:C9:08:41:DB 10:00:5A:F1:02:37 F4 OPENED
```

SAP value in hex (0FE)

El valor SAP de la sesión.

Interface

El número y tipo de interfaz a través de la cual se ejecuta la sesión.

Reply Timer (T1)

Indica el tiempo que tarda el temporizador en caducar cuando LLC no puede recibir un reconocimiento o una respuesta de otra estación LLC.

Receive ACK Timer (T2)

Indica el retardo de tiempo que LLC utiliza antes de enviar un reconocimiento para una trama I recibida.

Inactivity Timer (Ti)

Indica el tiempo que LLC espera durante la inactividad antes de emitir un RR.

MAX Retry Value (N2)

El número máximo de reintentos del protocolo LLC.

MAX I-field Size (N1)

Cantidad máxima de datos (en bytes) permitidos en el campo I de una trama LLC2.

Rcvd I-frame before ACK (N3)

Indica el valor que se utiliza con el temporizador T2 para reducir el tráfico de reconocimiento para tramas I recibidas.

Transmit Window Size (Tw)

Indica el número máximo de tramas I que se pueden enviar antes de recibir un RR.

Acks Needed to Inc Ww (Nw)

Este campo se establece en el valor por omisión 1.

Frames Xmt and Rcvd

Contador que visualiza el número total de tipos de tramas transmitidas (Xmt) y (Rcvd).

I-frames discarded by LLC

Contador que visualiza el número total de tramas I eliminadas por LLC, normalmente porque el número de secuencia está fuera de secuencia.

I-frames refused by LLC user

Contador que visualiza el número de tramas I eliminadas por el software superior al LLC. Por ejemplo, DLS (Conmutación de enlace de datos).

Cumulative number of sessions

El número total de sesiones que se han abierto en este SAP.

Number of active sessions

El número total de sesiones activas actualmente que están en ejecución en la interfaz.

Session ID (int-sap-id)

El ID de sesión para la interfaz de supervisión.

Local MAC

La dirección MAC del LLC del direccionador.

Remote MAC

La dirección MAC del LLC remoto.

Remote SAP

El SAP remoto de la conexión LLC.

Remote State

El estado o estados finitos que son el resultado de la interacción entre similares LLC. Hay 21 estados que se describen más abajo.

Link_Closed

El similar LLC remoto no se reconoce en el similar LLC local y se considera no existente.

Disconnected

El similar LLC local se reconoce en el otro similar. Este similar LLC puede enviar y recibir mandatos XID, TEST, SABME y DISC; y respuestas XID TEST, UA y DM.

Link_Opening

El estado del similar LLC local después de enviar un SABME o UA en respuesta a un SABME recibido.

Disconnecting

El estado del LLC local después de enviar un mandato DISC al similar LLC remoto.

FRMR_Sent

El similar LLC local ha entrado en el estado de excepción de rechazo de trama y ha enviado una respuesta FRMR a través del enlace.

Link_Opened

El similar LLC local está en la fase de transferencia de datos.

Local_Busy

El similar LLC local no puede recibir ninguna trama I adicional.

Supervisión de LLC

Rejection

Un similar LLC local ha recibido una o varias tramas I fuera de secuencia.

Checkpointing

El similar LLC local ha enviado un sondeo al similar LLC remoto y está esperando una respuesta adecuada.

CKPT_LB

Una combinación de los estados de checkpointing y local_busy.

CKPT_REJ

Una combinación de los estados de checkpointing y rejection.

Resetting

El similar LLC local ha recibido un SABME y está restableciendo el enlace.

Remote_Busy

El estado que se produce cuando se recibe un RNR del similar LLC remoto.

LB_RB

Una combinación de los estados de local_busy y remote_busy.

REJ_LB

Una combinación de estados de rejection y local_busy.

REJ_RB

Una combinación de estados de rejection y remote_busy.

CKPT_REJ_LB

Una combinación de estados de checkpointing, rejection y local_busy.

CKPT_CLR

Una combinación de estados resultante de la terminación de una condición local_busy mientras el similar LLC es CKPT_LB.

CKPT_REJ_CLR

Una combinación de estados resultante de la transferencia de un borrado de local_busy no confirmado mientras la estación de trabajo está en estado CKPT_REJ_LB.

REJ_LB_RB

Una combinación de los estados rejection, local_busy y remote_busy.

FRMR_Received

El similar LLC local ha recibido una respuesta FRMR del similar LLC remoto.

Session

Visualiza información sobre la sesión LLC especificada que está abierta en la interfaz.

Ejemplo:

```
list session
Session Id: [0]? 00-F4-0000

Interface0,           TKR/0
Remote MAC addr      10:00:5A:F1:02:37
Source MAC addr      00:00:C9:08:35:47
Remote SAP            F4
Local SAP             F4
RIF                   (089E 0101 0022 0010)
Access Priority       0
State                 LINK_OPENED
Replay Timer         1 sec
Receive ACK Timer (T2) 100 millisec
Inactivity Timer (Ti) 30 sec
MAX I-field Size (N1) 2052
MAX Retry Value (N2) 8
```

```

Rcvd I-frames before ACK (N3) 1
Transmit Window Size (Tw)      2
Working Transmit Size (Ww)     2
Acks Needed to Inc Ww (Nw)    1
Current Send Seq (Vs)         9
Current Rcv Seq (Vr)          7
Last ACK'd sent frame (Va)     9
No. of frames in ACK pend q    0
No. of frames in Tx pend q     0
Local Busy                     NO
Remote Busy                     NO
Poll Retry count               8
Appl output flow stopped      NO
Send process running          YES

```

```

Frame      Xmt  Rcvd
I-frames   1456 2678
RR-frames  502  403
RNR-frames 0    0
REJ-frames 0    0
I-frames discarded by LLC 0
I-frames Refused by LLC user 0

```

Session Id

Indica el número de ID de sesión.

Interface

Indica el número de la interfaz en la que se está ejecutando esta sesión.

Remote MAC addr

Indica la dirección MAC del similar LLC remoto.

Source MAC addr

Indica la dirección MAC del LLC local.

Remote SAP

El SAP de la parte remota de la conexión LLC.

Local SAP

El SAP de la parte local de la conexión LLC.

RIF El RIF real de la trama.

Access Priority

Prioridad del paquete. 07 para el control de capa superior.

State El estado o estados finitos que son el resultado de la interacción entre similares LLC. Consulte el mandato **list sap** en la página 255 para obtener más información.

Receive ACK timer (T2)

Indica el retardo de tiempo que LLC utiliza antes de enviar un reconocimiento para una trama I recibida.

Inactivity timer (Ti)

Indica el tiempo que LLC espera durante la inactividad antes de emitir un RR.

MAX I-field size (N1)

Tamaño máximo del campo de datos (en bytes) de una trama. El valor por omisión es el tamaño de la interfaz.

MAX Retry Value (N2)

El número máximo de veces que el LLC transmite un RR sin recibir ningún reconocimiento

Rcvd I-frames before ACK (N3)

Indica el valor que se utiliza con el temporizador T2 para reducir el tráfico de reconocimiento para tramas I recibidas.

Supervisión de LLC

Transmit window size (Tw)

Indica el número máximo de tramas I que pueden enviarse antes de recibir un RR.

Working transmit size (Ww)

El número máximo de tramas I que se envían antes de recibir un RR.

Acks Needed to Inc Ww (Nw)

Este campo se establece en el valor por omisión 1.

Current send seq (Vs)

Variable de estado de envío (valor Ns para la siguiente trama I que se va a transferir).

Current Rcv seq (Vr)

Variable de estado de recepción (siguiente Ns de la secuencia que va a aceptar).

Last ACK'd sent frame (Va)

Variable de estado reconocido (último Nr válido recibido).

No. of frames in ACK pend q

Número de tramas I transmitidas en espera de reconocimiento.

No. of frames in transmit pend q

Número de tramas en espera de transmisión.

Local Busy

La parte local de la conexión LLC está enviando RNR.

Remote Busy

La parte remota del LLC está recibiendo RNR.

Poll Retry count

Indica el valor actual del reintento del contador (cuenta abajo) del protocolo LLC.

Appl output flow stopped

El LLC ha indicado a la aplicación que deje de proporcionarle tramas de datos de salida.

Send process running

Este proceso se ejecuta simultáneamente con todas las demás acciones de trama y toma las tramas I de la cola de transmisión y las envía.

Frames Xmt and Rcvd

Visualiza el número total de tipos de tramas transmitidas (Xmt) y (Rcvd).

I-frames discarded by LLC

Contador que visualiza el número total de tramas I eliminadas por LLC, normalmente porque el número de secuencia está fuera de secuencia.

I-frames refused by LLC user

Contador que visualiza el número de tramas I eliminadas por el software superior al LLC. Por ejemplo, DLS (Conmutación de enlace de datos).

Set

Utilice el mandato **set** para configurar dinámicamente los parámetros LLC de una sesión LLC actual. Cualquier cambio que realice en los parámetros surtirá efecto durante la sesión. Estos parámetros son los mismos que los listados en la sección "Set" en la página 252.

Atención: El cambio de los valores por omisión de los parámetros LLC puede afectar a la forma en que funciona el protocolo LLC.

Sintaxis:

```

set                n2-max_retry cuenta
                    n3-frames-rcvd-before-ack cuenta
                    nw-acks-to-inc-ww cuenta
                    t1-reply-timer segundos
                    t2-receive-ack-timer segundos
                    ti-inactivity-timer segundos
                    tw-transmit-window segundos

```

n2-max_retry

El número máximo de reintentos del protocolo LLC. Por ejemplo, N2 es el número máximo de veces que el LLC transmite un RR sin recibir un reconocimiento cuando caduca el temporizador de inactividad. El valor por omisión es 8. El mínimo es 1. El máximo es 127.

n3-frames-rcvd-before-ack

Este valor se utiliza con el temporizador T2 para reducir el tráfico de reconocimientos para las tramas I recibidas. Establezca este contador en un valor especificado. Cada vez que se recibe una trama I, se reduce este valor. Cuando este contador llega a 0 o caduca el temporizador T2, se envía un reconocimiento. El valor por omisión es 1. El mínimo es 1. El máximo es 255.

nw-acks-to-inc-ww

Este campo se establece en el valor por omisión 1.

t1-reply-timer

Este temporizador caduca cuando LLC no puede recibir un reconocimiento o una respuesta necesarios de otra estación LLC. Cuando este temporizador caduca, se envía un RR con el bit de sondeo activado y se vuelve a iniciar T1. Si el LLC no recibe ninguna respuesta después del número máximo de reintentos configurados (N2), el enlace subyacente se declara no operativo. El valor por omisión es 1. El mínimo es 1. El máximo es 256.

t2-receive-ack-timer

Este temporizador se utiliza para retrasar el envío de un reconocimiento para una trama recibida en formato I. Este temporizador se inicia cuando se recibe una trama I y se restablece cuando se envía un reconocimiento. Si este temporizador caduca, LLC2 envía un reconocimiento lo antes posible. Establezca este valor de modo que sea inferior al de T1. Esto asegura que el similar LLC2 remoto reciba el reconocimiento retrasado antes de que caduque el temporizador T1. El valor por omisión es 1 (100 ms). El mínimo es 1. El máximo es 2560.

Supervisión de LLC

Nota: Si este temporizador se establece en 1 (el valor por omisión) no se ejecutará (por ejemplo, **n3-frames-rcvd-before-ack=1**).

ti-inactivity-timer

Este temporizador caduca cuando LLC no recibe ninguna trama durante un período de tiempo especificado. Cuando este temporizador caduca, el LLC transmite un RR hasta que otro LLC responde o el temporizador N2 caduca. El valor por omisión es de 30 segundos. El mínimo es 1 segundo. El máximo es 256 segundos.

tw-transmit-window

Establece el número máximo de tramas I que pueden enviarse antes de recibir un RR. Suponiendo que el otro extremo de la sesión LLC pueda realmente recibir esta cantidad de tramas I consecutivas y que el direccionador tenga suficiente memoria de almacenamiento dinámico para conservar copias de estas tramas hasta que se reciba un reconocimiento, si se incrementa este valor puede incrementarse la productividad. El valor por omisión es 2. El mínimo es 1. El máximo es 127.

Capítulo 19. Utilización de la interfaz de red Ethernet

Este capítulo describe cómo utilizar la interfaz Ethernet. Incluye la sección “Visualización de estadísticas Ethernet mediante el mandato interface”.

Visualización de estadísticas Ethernet mediante el mandato interface

También puede utilizar el mandato **interface** desde el entorno GWCON para visualizar las estadísticas siguientes.

```
+ interface 4
Nt Nt' Interface Slot-Port Self-Test Self-Test Maintenance
4 4 Eth/0 Slot: 4 Port: 1 Passed Failed Failed
Ethernet/IEEE 802.3 MAC/data-link on Ethernet interface
Physical address AA0004000318
PROM address 10005AFF0016
Microcode Level Uu17c

Input statistics:
failed, packet too long 0 failed, CRC error 1
failed, alignment error 0 failed, FIFO over-run 0
buffer full warnings 0 packets missed 1
internal mac rx errors 0

Output statistics:
initially deferred 12 single collision 1
multiple collisions 1 total collisions 4
failed, excess collisions 0 failed, FIFO under-run 0
failed, carrier check 0 CD heartbeat error 0
```

Estas estadísticas tienen el significado siguiente:

Nt Número de red global.

Nt' Este campo es para la tarjeta de interfaz serie. Descarte la salida.

Interface

El nombre de interfaz y su número de instancia.

Port Número de puerto

Slot Número de ranura

Self-Test: Passed

Número de autopruebas que han sido satisfactorias.

Self-Test: Failed

Número de autopruebas que han fallado.

Maintenance: Failed

Número de anomalías de mantenimiento.

Physical address

La dirección Ethernet del dispositivo que se utiliza actualmente. Puede ser la dirección PROM o una dirección sobregabada por otro protocolo.

PROM address

La dirección Ethernet exclusiva y permanente en la PROM para esta interfaz Ethernet.

Input statistics:

failed, packet too long o failed, frame too long

Se incrementa el contador Failed, Packet Too Long cuando la interfaz

Utilización de las interfaces de red Ethernet

recibe un paquete que es mayor que el tamaño máximo de 1518 bytes para una trama Ethernet. Estos datos se exportan mediante SNMP como el contador dot3StatsFrameTooLongs.

failed, CRC error o failed, FCS (Frame Check Sequence) error

Se incrementa el contador Failed, CRC (Cyclic Redundancy Check) Error cuando la interfaz recibe un paquete con un error CRC. Estos datos se exportan mediante SNMP como el contador dd3StatsFCSErrors.

failed, framing error o failed, alignment error

Se incrementa el contador Failed, Framing Error cuando la interfaz recibe un paquete cuya longitud en bits no es un múltiplo de ocho.

failed, FIFO over-run o failed, FIFO overrun

Se incrementa el contador Failed, FIFO (First In, First Out) Overrun cuando el conjunto de chips Ethernet no puede almacenar bytes en el almacenamiento intermedio de paquetes local a la velocidad a la que salen del cable.

buffer full warnings

El contador Buffer Full Warnings se incrementa cada vez que el almacenamiento intermedio de paquetes local está lleno.

packets missed

El contador Packets Missed se incrementa cuando la interfaz intenta recibir un paquete, pero el almacenamiento intermedio de paquetes local está lleno. Este error indica que la red tiene más tráfico del que la interfaz puede manejar.

internal mac rcv errors

Errores de recepción que no son por llegar tarde, ser excesivo o por colisiones de comprobación de portadora. Estos datos se exportan mediante SNMP como el contador dot3StatsInternalMacReceiveErrors. Esta estadística es la suma de los desbordamientos FIFO.

Output statistics:

initially deferred o deferred transmission

El contador Initially Deferred se incrementa cuando el mecanismo de detección de portadora detecta una actividad de línea que hace que la interfaz diferiera la transmisión. Estos datos se exportan mediante SNMP como el contador dot3StatsDeferredTransmissions.

single collision

El contador Single Collision se incrementa cuando un paquete tiene una colisión en el primer intento de transmisión y, después, se envía satisfactoriamente el paquete en el segundo intento de transmisión. Estos datos se exportan mediante SNMP como el contador dot3StatsSingleCollisionFrames.

multiple collisions

El contador Multiple Collisions se incrementa cuando un paquete tiene múltiples colisiones antes de transmitirse satisfactoriamente. Estos datos se exportan mediante SNMP como el contador dot3MultipleCollisionFrames.

total collisions

El contador Total Collisions se incrementa por el número de colisiones en que incurre un paquete.

failed, excess collisions

El contador Failed, Excess Collisions se incrementa cuando falla la transmisión de un paquete debido a 16 colisiones sucesivas. Este error

Utilización de las interfaces de red Ethernet

indica un alto volumen de tráfico de red o problemas de hardware con la red. Estos datos se exportan mediante SNMP como el contador dot3StatsExcessiveCollisions.

failed, FIFO underrun

El contador Failed, FIFO Underrun se incrementa cuando la transmisión de paquetes falla debido a que la interfaz no puede recuperar paquetes del almacenamiento intermedio de paquetes local con suficiente rapidez para transmitirlos a la red.

failed, carrier check o failed, carrier sense error

El contador Failed, Carrier Check se incrementa cuando un paquete colisiona porque la detección de portadora está inhabilitada. Este error indica un problema entre la interfaz y su transceptor Ethernet. Estos datos se exportan mediante SNMP como el contador dot3StatsCarrierSenseErrors.

CD heartbeat error o SQE test error

El contador CD (Collision Detection) Heartbeat Error o SQE (Signal Quality Error) se incrementa cuando la interfaz envía un paquete pero detecta que el transceptor no da señales de actividad. El paquete se trata como si se hubiese transmitido satisfactoriamente porque algunos transceptores no generan señales de actividad. Estos datos se exportan mediante SNMP como el contador dot3StatsSQETestErrors.

Utilización de las interfaces de red Ethernet

Capítulo 20. Configuración y supervisión de la interfaz de red Ethernet

Este capítulo describe los mandatos operativos y de configuración de interfaces Ethernet. Incluye las secciones siguientes:

- “Acceso al proceso operativo de la interfaz Ethernet” en la página 269
- “Mandatos de supervisión de interfaz Ethernet” en la página 269
- “Soporte para la reconfiguración dinámica de Ethernet” en la página 270

Acceso al proceso de configuración de interfaces Ethernet

Utilice el procedimiento siguiente para acceder al proceso de configuración. Este proceso le proporciona acceso al proceso de *configuración* de una interfaz Ethernet.

1. En el indicador OPCON, entre **talk 6**. (Para ver más detalles de este mandato, consulte la sección “¿Qué es el proceso OPCON?” en la página 33.) Por ejemplo:

```
* talk 6
Config>
```

Se visualiza el indicador CONFIG (Config>) en la consola. Si no aparece el indicador cuando entre en la configuración, pulse **Intro** de nuevo.

2. En el indicador CONFIG, entre el mandato **list devices** para visualizar los números de interfaces de red para las que el direccionador está configurado actualmente.
3. Anote los números de interfaz.
4. Entre el mandato **network** y el número de la interfaz Ethernet que desea configurar. Por ejemplo:

```
Config> network 0
ETH Config>
```

Se visualiza el indicador de configuración Ethernet (ETH Config>).

Mandatos de configuración Ethernet

Esta sección resume y explica los mandatos de configuración Ethernet. Entre los mandatos en el indicador ETH config>.

Tabla 33. Resumen de los mandatos de configuración de Ethernet

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página 10.
Connector-Type	Establece el tipo de conector.
IP-Encapsulation	Establece la encapsulación IP como Ethernet (tipo X'0800'), como IEEE (802.3 con SNAP) o como ambos.
List	Visualiza el tipo de conector actual, la encapsulación NetWare IPX y la encapsulación IP.
Physical-Address	Establece la dirección MAC física.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página 11.

Mandatos de configuración Ethernet (Talk 6)

Connector-Type

Utilice el mandato **connector-type** para establecer el tipo de conector. Los 2216 soportan los conectores AUI (10BASE5) y RJ-45 (10BASE-T) y las opciones de configuración automática.

Sintaxis:

connector-type *name*

IP-Encapsulation

Utilice el mandato **IP-encapsulation** para seleccionar Ethernet (Ethernet tipo X'0800'), IEEE 802.3 (Ethernet 802.3 con SNAP) o ambos. El valor por omisión es Ethernet.

La opción **both** permite que el 2216 utilice la encapsulación Ethernet para transmitir a los sistemas principales que tienen encapsulación Ethernet y utilizar la encapsulación IEEE 802.3 para transmitir a los sistemas principales que tienen encapsulación IEEE 802.3. Si la LAN Ethernet incluye unos sistemas principales que utilizan un tipo de encapsulación y otros que utilizan el otro, si se entra **both** permite que todos ellos se comuniquen.

La opción **both** sólo se aplica a las tramas de vertimiento único. Si entra **both**, se le solicita que entre **ethernet** o **ieee-802.3** para las tramas de difusión o de multidifusión.

Sintaxis:

IP-encapsulation

- **ethernet**
- **ieee-802.3**
- **both**

Ejemplo:

```
Eth Config [1]>ip-encapsulation both
How would you like IP broadcast/multicast frames to be sent (ETHER/IEEE-802.3) [ETHER]?
```

List

Utilice el mandato **list** para visualizar la configuración actual para la interfaz Ethernet, incluyendo el tipo de conector, el tipo de encapsulación IPX y el tipo de encapsulación IP.

Sintaxis:

list *all*

Ejemplo:

```
list all
Connector type:      AUI (10BASE5)
IP Encapsulation:   ETHER
MAC Address:        023456789A56
```

Physical-Address

Utilice el mandato **physical-address** para establecer la dirección física (MAC).

Sintaxis: **physical-address** *dirección*

Mandatos de configuración Ethernet (Talk 6)

physical-address

Este mandato le permite indicar si desea definir una dirección administrada localmente para la dirección de subcapa MAC de la interfaz Ethernet o utilizar la dirección por omisión incorporada (indicada por sólo ceros). La dirección de subcapa MAC es la dirección que la interfaz Ethernet utiliza para recibir y transmitir tramas.

Nota: Si se pulsa **Intro** el valor se deja igual. Si se entra **0**, el direccionador utiliza la dirección incorporada. El valor por omisión es utilizar la dirección incorporada.

Valores válidos: Cualquier dirección hexadecimal de 12 dígitos.

Valor por omisión: dirección incorporada (indicada por sólo ceros).

Ejemplo:

physical-address

MAC address in 00:00:00:00:00:00 form []? 12:15:00:FA:00:FE

Acceso al proceso operativo de la interfaz Ethernet

Para supervisar la información relacionada con la Interfaz de red Ethernet, acceda al proceso de supervisión de la interfaz llevando a cabo lo siguiente:

1. En el indicador OPCON, entre **talk 5**. Por ejemplo:

```
* talk 5
```

Se visualiza el indicador GWCON (+) en la consola. Si no aparece el indicador cuando entre en GWCON, pulse **Intro** de nuevo.

2. En el indicador GWCON, entre el mandato **configuration** para ver los protocolos y las redes para los que está configurado el direccionador. Por ejemplo:

```
+ configuration
```

Consulte la página “Configuration” en la página 120 para ver un ejemplo de salida del mandato **configuration**.

3. Entre el mandato **network** y el número de la interfaz Ethernet. En este ejemplo:

```
+ network 0  
ETH>
```

Se visualiza el indicador de supervisión Ethernet. Ahora, puede ver la información acerca de la interfaz Ethernet entrando los mandatos de supervisión.

Mandatos de supervisión de interfaz Ethernet

Esta sección resume y explica los mandatos de supervisión Ethernet. Entre los mandatos en el indicador ETH>. La Tabla 34 lista los mandatos de supervisión.

Tabla 34. Resumen de los mandatos de supervisión Ethernet

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página 10.

Mandatos de supervisión de interfaz Ethernet (Talk 5)

Tabla 34. Resumen de los mandatos de supervisión Ethernet (continuación)

Mandato	Función
Collisions	Visualiza las estadísticas de colisión para la interfaz Ethernet especificada.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página 11.

Collisions

Este mandato muestra las cuentas de transmisiones para los paquetes que han incurrido en colisiones antes de una transmisión satisfactoria. Se proporcionan contadores para los paquetes enviados después de 15 colisiones. El aumento en el número de transmisiones de paquetes con colisiones y números altos de colisión por paquete son signos de la transmisión en una Ethernet ocupada.

El mandato **clear** de OPCON borra estos contadores. Estos datos se exportan mediante SNMP como el contador dot3CollTable.

Sintaxis:

collisions

Ejemplo:

```
Eth> coll
Transmitted with 1 collisions:0
Transmitted with 2 collisions:0
Transmitted with 3 collisions:0
Transmitted with 4 collisions:0
Transmitted with 5 collisions:0
Transmitted with 6 collisions:0
Transmitted with 7 collisions:0
Transmitted with 8 collisions:0
Transmitted with 9 collisions:0
Transmitted with 10 collisions:0
Transmitted with 11 collisions:0
Transmitted with 12 collisions:0
Transmitted with 13 collisions:0
Transmitted with 14 collisions:0
Transmitted with 15 collisions:0
```

Soporte para la reconfiguración dinámica de Ethernet

Esta sección describe la reconfiguración dinámica (DR) en la medida en que afecta a los mandatos Talk 6 y Talk 5.

Delete Interface de CONFIG (Talk 6)

Ethernet soporta el mandato **delete interface** de CONFIG (Talk 6) sin ninguna restricción.

Activate Interface de GWCON (Talk 5)

Ethernet soporta el mandato **activate interface** de GWCON (Talk 5) sin ninguna restricción.

El mandato **activate interface** de GWCON (Talk 5) soporta todos los mandatos específicos de interfaz Ethernet.

Reset Interface de GWCON (Talk 5)

Ethernet soporta el mandato **reset interface** de GWCON (Talk 5) sin ninguna restricción.

El mandato **reset interface** de GWCON (Talk 5) soporta todos los mandatos específicos de interfaz Ethernet.

Capítulo 21. Utilización de la interfaz de red Ethernet de 10/100 Mbps

Este capítulo describe cómo utilizar la interfaz Ethernet de 10/100 Mbps . Incluye las secciones siguientes:

- “Visualización de estadísticas Ethernet de 10/100 Mbps”
- “Negociación automática en la interfaz Ethernet de 10/100 Mbps” en la página 281
- “Configuración de valores distintos de automático para dúplex” en la página 281
- “Configuraciones que pueden resultar en una anomalía de la activación del enlace en el IBM 2216” en la página 281
- “Configuraciones que pueden resultar en discrepancias de las modalidades de dúplex durante el funcionamiento” en la página 282

Visualización de estadísticas Ethernet de 10/100 Mbps

Puede utilizar el mandato **interface** desde el entorno GWCON para visualizar las estadísticas siguientes.

```
+i 0
Net  Net'  Interface  Slot-Port          Self-Test  Self-Test  Maintenance
0    0      Eth/0      Slot: 1  Port: 1          Passed    Failed    Failed
                                1          0          0

Ethernet/IEEE 802.3 MAC/data-link on 10/100-Ethernet interface

Encapsulation type      Ethernet
Physical address        002035030008
PROM address            002035030008
Actual address          002035030008
Adapter Level           0
Configured Duplex:      Auto-Negotiation
Actual Duplex:          Half Duplex
Configured Speed:       Auto-Negotiation
Actual Speed:           100 Mbps

Input statistics:
failed, packet too long      0  failed, CRC error          0
failed, alignment error      0  failed, receive overflow    0
*receive collision           0  *missed frame              0
**frames filtered            0  receive underrun           0
receive error                 0

Output statistics:
one retry                     0  single collision            0
multiple collisions           0  failed, transmit underflow  0
failed, excess collisions     0  failed, loss of carrier     0
late collisions               0  more than one retry         0
buffer error                  0  total collisions            0
excessive deferral           0  deferred                    0
memory error                  0

Connection statistics:
disconnects                   0  false carrier sense        0

* cannot be cleared.
** cleared automatically when read.
```

Estas estadísticas tienen el significado siguiente:

Nt Número de red global.

Nt' Este campo es para la tarjeta de interfaz serie. Descarte la salida.

Interface

El nombre de interfaz y su número de instancia.

Utilización de interfaces de red Ethernet de 10/100 Mbps

Self-Test: Passed

Número de autopruebas que han sido satisfactorias.

Self-Test: Failed

Número de autopruebas que han fallado.

Maintenance: Failed

Número de anomalías de mantenimiento.

Physical address

La dirección Ethernet del dispositivo que se utiliza actualmente. Puede ser la dirección PROM o una dirección sobregabada por otro protocolo.

PROM address

La dirección Ethernet exclusiva y permanente en la PROM para esta interfaz Ethernet.

Link Status

El estado actual del enlace, activado o desactivado.

Configured duplex

El valor configurado para dúplex. Los valores pueden ser Half Duplex, Full Duplex o Auto-Negotiation. Este valor sólo se aplica a la Ethernet de 10/100 Mbps.

Actual duplex

El valor al que está funcionando el adaptador actualmente. Puede ser diferente del valor configurado, dependiendo de la posibilidad del conmutador. Si el adaptador no está activado, el valor visualizado será *Unknown*. De lo contrario, el valor puede ser Half Duplex o Full Duplex.

Siempre que el asociado del enlace (conmutador o concentrador) no participe durante la fase de negociación, aparecerá *** después del valor real de modalidad de dúplex. Cuando se indica ***, debe verificarse el valor del dúplex operativo en el conmutador o concentrador para la coherencia.

La mayoría de concentradores (a diferencia de los conmutadores) sólo pueden soportar la modalidad de semi-dúplex y no tienen capacidad de negociación. Por lo tanto, normalmente se visualizará la indicación *** cuando la interfaz esté conectada a un concentrador.

También se anotará cronológicamente un mensaje mediante el sistema ELS siempre que exista una posibilidad de discrepancia en la modalidad dúplex.

Nota: Si el asociado del enlace (conmutador o concentrador) al que la interfaz está conectado no responde durante la fase de negociación, puede dar como resultado que los dos funcionen con diferentes modalidades de dúplex. Es decir, la interfaz puede estar funcionando en semi-dúplex, mientras que el puerto de conmutador esté funcionando en modalidad de dúplex. Una discrepancia en la modalidad de dúplex puede dar como resultado una grave degradación del rendimiento. Consulte la sección "Mandatos de configuración de Ethernet de 10/100-Mbps" en la página 285 para obtener información importante en relación a las configuraciones de dúplex y de velocidad.

Configured speed

El valor configurado para la velocidad. Los valores pueden ser 10 Mbps, 100 Mbps o negociación automática.

Utilización de interfaces de red Ethernet de 10/100 Mbps

Actual speed

La velocidad a la que funciona actualmente el adaptador. Si el adaptador no está activado, el valor visualizado será *Unknown*. De lo contrario, el valor puede ser 10 Mbps o 100 Mbps .

Input statistics:

failed, packet too long o failed, frame too long

Se incrementa el contador Failed, Packet Too Long cuando la interfaz recibe un paquete que es mayor que el tamaño máximo de 1518 bytes para una trama Ethernet. Estos datos se exportan mediante SNMP como el contador dot3StatsFrameTooLongs.

failed, CRC error o failed, FCS (Frame Check Sequence) error

Se incrementa el contador Failed, CRC (Cyclic Redundancy Check) Error cuando la interfaz recibe un paquete con un error CRC. Estos datos se exportan mediante SNMP como el contador dd3StatsFCSErrors.

failed, alignment error

El contador Failed, Framing Error se incrementa cuando la interfaz recibe un paquete en el que la longitud en bits no es un múltiplo de ocho. Este valor sólo se aplica a la Ethernet de 10/100 Mbps.

failed, receive overflow

El error de desbordamiento indica que el receptor ha perdido toda o parte de la trama de entrada, debido a la imposibilidad de mover los datos de FIFO de recepción al almacenamiento intermedio de memoria antes de que el FIFO interno se desbordase.

receive collision

Indica el número total de colisiones encontradas por el soporte receptor en el adaptador.

Nota: El mandato **clear statistics** no puede borrar este contador porque se mantiene en el adaptador. El mandato **test network** es la única manera de restablecer este contador.

missed frame

Indica el número de tramas de recepción de entrada perdidas debido a la no disponibilidad de un almacenamiento intermedio de recepción en el sistema. Este error indica que el sistema no está procesando las tramas recibidas a la misma velocidad que se reciben de la red local.

Nota: El mandato **clear statistics** no puede borrar este contador porque se mantiene en el adaptador. El mandato **test network** es la única manera de restablecer este contador.

frames filtered

Indica el número de tramas de entrada que el adaptador ha eliminado. Este contador sólo se actualiza cuando el puente está habilitado.

Nota: Este contador se mantiene en el adaptador y se borra cada vez que se lee. Los mandatos **interface statistics** y **test network** borrarán este contador.

receive underrun

Indica el número de veces que el adaptador no ha tenido un segundo almacenamiento intermedio para almacenar una trama larga (que necesita más de un almacenamiento intermedio).

Utilización de interfaces de red Ethernet de 10/100 Mbps

receive error

Este contador de hardware se incrementa con cada paquete en el que se detecta un error de recepción. Si hay una o varias condiciones de error del receptor durante una recepción válida de paquetes (es decir, si no se ha producido ninguna colisión durante la recepción de paquetes), el contador se incrementa una vez al final de la recepción de paquetes.

Output statistics:

single collision

El contador Single Collision se incrementa cuando un paquete tiene una colisión en el primer intento de transmisión y, después, se envía satisfactoriamente el paquete en el segundo intento de transmisión. Estos datos se exportan mediante SNMP como el contador dot3StatsSingleCollisionFrames. Este valor sólo se aplica a la Ethernet de 10/100 Mbps.

multiple collisions

El contador Multiple Collisions se incrementa cuando un paquete tiene múltiples colisiones antes de transmitirse satisfactoriamente. Estos datos se exportan mediante SNMP como el contador dot3MultipleCollisionFrames. Este valor sólo se aplica a la Ethernet de 10/100 Mbps.

failed, transmit underflow

La pérdida de datos de transmisión indica que el transmisor ha truncado un mensaje porque no podía leer los datos de la memoria con la suficiente rapidez. También indica que el FIFO del adaptador se ha vaciado antes de llegar al final de la trama. IFO en almacenamiento intermedio de memoria antes de que el FIFO interno se desbordase.

failed, excess collisions

El contador Failed, Excess Collisions se incrementa cuando falla la transmisión de un paquete debido a 16 colisiones sucesivas. Este error indica un alto volumen de tráfico de red o problemas de hardware con la red. Estos datos se exportan mediante SNMP como el contador dot3StatsExcessiveCollisions. Este valor sólo se aplica a la Ethernet de 10/100 Mbps.

failed, loss of carrier

La pérdida de portadora se establece cuando se pierde la portadora durante la transmisión. El adaptador no reintenta en una condición de pérdida de portadora. Continuará transmitiendo toda la trama hasta que termine.

late collisions

Una colisión tardía indica que se ha producido una colisión después de que haya transcurrido el primer período el tiempo del canal. El adaptador no efectúa un reintento en condiciones de colisiones tardías.

more than one retry

Más de un reintento indica que se ha necesitado más de un reintento para transmitir una trama.

buffer error

El error de almacenamiento intermedio se produce si hay un problema de memoria dañada en el sistema o bajo determinadas condiciones de subdesbordamiento FIFO en el adaptador.

total collisions

El contador Total Collisions se incrementa por el número de colisiones en que incurre un paquete.

Utilización de interfaces de red Ethernet de 10/100 Mbps

excessive deferral

El aplazamiento excesivo indica que el transmisor del adaptador ha experimentado un Aplazamiento excesivo en esta trama de transmisión, donde Aplazamiento excesivo se define en el estándar de ISO 8802-3 (IEEE/ANSI 802.3).

deferred

Diferido indica el número de veces que el adaptador ha tenido que diferir al intentar transmitir una trama. Esta condición se produce si el canal DMA está ocupado cuando el adaptador está preparado para transmitir.

memory error

Los errores de memoria se producen cuando el adaptador no tiene acceso al bus de interfaz del sistema dentro del período programable de tiempo. Este error se producirá normalmente durante las operaciones de transmisión, indicando una pérdida de datos por defecto en la transmisión.

Connection statistics

disconnects

Indica el número de veces que la interfaz y su asociado en el enlace (conmutador o concentrador) se han desconectado entre si.

false carrier sense

Indica el número de veces que la interfaz ha encontrado un suceso de portadora falsa. El contador se inmoviliza cuando está lleno (a X'FFFF').

Estas estadísticas tienen el significado siguiente:

Nt Número de red global.

Nt' Este campo es para la tarjeta de interfaz serie. Descarte la salida.

Interface

El nombre de interfaz y su número de instancia.

Self-Test: Passed

Número de autopruebas que han sido satisfactorias.

Self-Test: Failed

Número de autopruebas que han fallado.

Maintenance: Failed

Número de anomalías de mantenimiento.

Physical address

La dirección Ethernet del dispositivo que se utiliza actualmente. Puede ser la dirección PROM o una dirección sobregabada por otro protocolo.

PROM address

La dirección Ethernet exclusiva y permanente en la PROM para esta interfaz Ethernet.

Actual address

Configured duplex

El valor configurado para dúplex. Los valores pueden ser Half Duplex, Full Duplex o Auto-Negotiation. Este valor sólo se aplica a la Ethernet de 10/100 Mbps.

Actual duplex

El valor al que está funcionando el adaptador actualmente. Puede ser diferente del valor configurado, dependiendo de la posibilidad del

Utilización de interfaces de red Ethernet de 10/100 Mbps

conmutador. Si el adaptador no está activado, el valor visualizado será *Unknown*. De lo contrario, el valor puede ser Half Duplex o Full Duplex.

Siempre que el asociado del enlace (conmutador o concentrador) no participe durante la fase de negociación, aparecerá *** después del valor real de modalidad de dúplex. Cuando se indica ***, debe verificarse el valor del dúplex operativo en el conmutador o concentrador para la coherencia.

La mayoría de concentradores (a diferencia de los conmutadores) sólo pueden soportar la modalidad de semi-dúplex y no tienen capacidad de negociación. Por lo tanto, normalmente se visualizará la indicación *** cuando la interfaz esté conectada a un concentrador.

También se anotará cronológicamente un mensaje mediante el sistema ELS siempre que exista una posibilidad de discrepancia en la modalidad dúplex.

Nota: Si el asociado del enlace (conmutador o concentrador) al que la interfaz está conectado no responde durante la fase de negociación, puede dar como resultado que los dos funcionen con diferentes modalidades de dúplex. Es decir, la interfaz puede estar funcionando en semi-dúplex, mientras que el puerto de conmutador esté funcionando en modalidad de dúplex. Una discrepancia en la modalidad de dúplex puede dar como resultado una grave degradación del rendimiento. Consulte la sección “Mandatos de configuración de Ethernet de 10/100-Mbps” en la página 285 para obtener información importante en relación a las configuraciones de dúplex y de velocidad.

Configured speed

El valor configurado para la velocidad. Los valores pueden ser de 10 Mbps, 100 Mbps o negociación automática. Este valor sólo se aplica a la Ethernet de 10/100 Mbps.

Actual speed

La velocidad a la que funciona actualmente el adaptador. Si el adaptador no está activado, el valor visualizado será *Unknown*. De lo contrario, el valor puede ser 10 Mbps o 100 Mbps .

Input statistics:

failed, packet too long o failed, frame too long

Se incrementa el contador Failed, Packet Too Long cuando la interfaz recibe un paquete que es mayor que el tamaño máximo de 1518 bytes para una trama Ethernet. Estos datos se exportan mediante SNMP como el contador dot3StatsFrameTooLongs.

failed, CRC error o failed, FCS (Frame Check Sequence) error

Se incrementa el contador Failed, CRC (Cyclic Redundancy Check) Error cuando la interfaz recibe un paquete con un error CRC. Estos datos se exportan mediante SNMP como el contador dd3StatsFCSErrors.

failed, alignment error

El contador Failed, Framing Error se incrementa cuando la interfaz recibe un paquete en el que la longitud en bits no es un múltiplo de ocho. Este valor sólo se aplica a la Ethernet de 10/100 Mbps.

failed, receive overflow

El error de desbordamiento indica que el receptor ha perdido toda o parte

Utilización de interfaces de red Ethernet de 10/100 Mbps

de la trama de entrada, debido a la imposibilidad de mover los datos de FIFO de recepción al almacenamiento intermedio de memoria antes de que el el FIFO interno se desbordase.

receive collision

Indica el número total de colisiones encontradas por el soporte receptor en el adaptador.

Nota: El mandato **clear statistics** no puede borrar este contador porque se mantiene en el adaptador. El mandato **test network** es la única manera de restablecer este contador.

missed frame

Indica el número de tramas de recepción de entrada perdidas debido a la no disponibilidad de un almacenamiento intermedio de recepción en el sistema. Este error indica que el sistema no está procesando las tramas recibidas a la misma velocidad que se reciben de la red local.

Nota: El mandato **clear statistics** no puede borrar este contador porque se mantiene en el adaptador. El mandato **test network** es la única manera de restablecer este contador.

frames filtered

Indica el número de tramas de entrada que el adaptador ha eliminado. Este contador sólo se actualiza cuando el puente está habilitado.

Nota: Este contador se mantiene en el adaptador y se borra cada vez que se lee. Los mandatos **interface statistics** y **test network** borrarán este contador.

receive underrun

Indica el número de veces que el adaptador no ha tenido un segundo almacenamiento intermedio para almacenar una trama larga (que necesita más de un almacenamiento intermedio).

receive error

Este contador de hardware se incrementa con cada paquete en el que se detecta un error de recepción. Si hay una o varias condiciones de error del receptor durante una recepción válida de paquetes (es decir, si no se ha producido ninguna colisión durante la recepción de paquetes), el contador se incrementa una vez al final de la recepción de paquetes.

Output statistics:

one retry

Indica que se ha necesitado exactamente un reintento para transmitir una trama. Estos datos se exportan mediante SNMP como el contador dot3StatsDeferredTransmissions. Este valor sólo se aplica a la Ethernet de 10/100 Mbps.

single collision

El contador Single Collision se incrementa cuando un paquete tiene una colisión en el primer intento de transmisión y, después, se envía satisfactoriamente el paquete en el segundo intento de transmisión. Estos datos se exportan mediante SNMP como el contador dot3StatsSingleCollisionFrames. Este valor sólo se aplica a la Ethernet de 10/100 Mbps.

multiple collisions

El contador Multiple Collisions se incrementa cuando un paquete tiene

Utilización de interfaces de red Ethernet de 10/100 Mbps

múltiples colisiones antes de transmitirse satisfactoriamente. Estos datos se exportan mediante SNMP como el contador dot3MultipleCollisionFrames. Este valor sólo se aplica a la Ethernet de 10/100 Mbps.

failed, transmit underflow

La pérdida de datos de transmisión indica que el transmisor ha truncado un mensaje porque no podía leer los datos de la memoria con la suficiente rapidez. También indica que el FIFO del adaptador se ha vaciado antes de llegar al final de la trama. IFO en almacenamiento intermedio de memoria antes de que el FIFO interno se desbordase.

failed, excess collisions

El contador Failed, Excess Collisions se incrementa cuando falla la transmisión de un paquete debido a 16 colisiones sucesivas. Este error indica un alto volumen de tráfico de red o problemas de hardware con la red. Estos datos se exportan mediante SNMP como el contador dot3StatsExcessiveCollisions. Este valor sólo se aplica a la Ethernet de 10/100 Mbps.

failed, loss of carrier

La pérdida de portadora se establece cuando se pierde la portadora durante la transmisión. El adaptador no reintenta en una condición de pérdida de portadora. Continuará transmitiendo toda la trama hasta que termine.

late collisions

Una colisión tardía indica que se ha producido una colisión después de que haya transcurrido el primer período el tiempo del canal. El adaptador no efectúa un reintento en condiciones de colisiones tardías.

more than one retry

Más de un reintento indica que se ha necesitado más de un reintento para transmitir una trama.

buffer error

El error de almacenamiento intermedio se produce si hay un problema de memoria dañada en el sistema o bajo determinadas condiciones de subdesbordamiento FIFO en el adaptador.

total collisions

El contador Total Collisions se incrementa por el número de colisiones en que incurre un paquete.

excessive deferral

El aplazamiento excesivo indica que el transmisor del adaptador ha experimentado un Aplazamiento excesivo en esta trama de transmisión, donde Aplazamiento excesivo se define en el estándar de ISO 8802-3 (IEEE/ANSI 802.3).

deferred

Diferido indica el número de veces que el adaptador ha tenido que diferir al intentar transmitir una trama. Esta condición se produce si el canal DMA está ocupado cuando el adaptador está preparado para transmitir.

memory error

Los errores de memoria se producen cuando el adaptador no tiene acceso al bus de interfaz del sistema dentro del período programable de tiempo. Este error se producirá normalmente durante las operaciones de transmisión, indicando una pérdida de datos por defecto en la transmisión.

Connection statistics

Utilización de interfaces de red Ethernet de 10/100 Mbps

disconnects

Indica el número de veces que la interfaz y su asociado en el enlace (conmutador o concentrador) se han desconectado entre sí.

false carrier sense

Indica el número de veces que la interfaz ha encontrado un suceso de portadora falsa. El contador se inmoviliza cuando está lleno (a X'FFFF').

Negociación automática en la interfaz Ethernet de 10/100 Mbps

La especificación de valores distintos de *automático* para la velocidad o dúplex en la interfaz Ethernet de 10/100 Mbps o su asociado en el enlace (puerto de conmutador) puede dar como resultado una discrepancia en la modalidad de dúplex o anomalías en la activación del enlace.

Las anomalías en la activación de enlaces debidas a las discrepancias de configuración se producirán en el IBM 2216 siempre que la velocidad configurada en ambos extremos no sea idéntica.

Cuando el valor de velocidad o de dúplex sea *negociación automática*, la velocidad y el dúplex se negociarán con el asociado de enlace y se utilizará su velocidad o dúplex configurados.

Configuración de valores distintos de automático para dúplex

Las interfaces Ethernet de 10/100 Mbps del IBM 2216 le avisarán siempre que haya la posibilidad de una discrepancia en la modalidad de dúplex entre el conmutador y el direccionador. Cuando no esté configurada la negociación automática en ambos extremos, no hay ninguna manera definida para que cada extremo determine la modalidad de dúplex que se utiliza en el extremo remoto y el conmutador y la interfaz de direccionador pueden funcionar con modalidades de dúplex que no sean idénticas.

Dependiendo de la implementación del conmutador, el puerto de conmutador puede funcionar a semi-dúplex, cuando el usuario haya configurado dúplex. Así, siempre existe la posibilidad de que se produzca una discrepancia entre el puerto de conmutador y la interfaz de direccionador. El IBM 2216 le avisará siempre que exista esa posibilidad, pero algunos conmutadores no proporcionan esa indicación.

Configuraciones que pueden resultar en una anomalía de la activación del enlace en el IBM 2216

La causa principal de la anomalía de la activación del enlace es la discrepancia en las velocidades.

Para evitar una anomalía en la activación del enlace, configure *auto* para la velocidad y el dúplex en el IBM 2216 y el puerto del conmutador.

Nota: Los resultados pueden variar dependiendo del fabricante y el modelo del conmutador.

Utilización de interfaces de red Ethernet de 10/100 Mbps

Tabla 35. Configuraciones que pueden resultar en anomalía de enlace en el IBM 2216

IBM 2216	Hub/Switch
Auto 10	HDX* 100
Auto 10	FDX* 100
Auto 100	HDX 10
Auto 100	FDX 10
HDX 10	HDX 100
HDX 10	FDX 100
HDX 100	HDX 10
HDX 100	FDX 10
FDX 10	HDX 100
FDX 10	FDX 100
FDX 100	HDX 10
FDX 100	FDX 10

* HDX = Semi-dúplex FDX = Dúplex

Configuraciones que pueden resultar en discrepancias de las modalidades de dúplex durante el funcionamiento

La causa principal de discrepancias de las modalidades de dúplex es la inhabilitación de la negociación automática en el puerto del conmutador y/o en la interfaz del IBM 2216.

Para evitar discrepancias en la modalidad de dúplex, configure *auto* para la velocidad y el dúplex en el IBM 2216 y en el puerto del conmutador.

Nota: Los resultados pueden variar dependiendo del fabricante y el modelo del conmutador.

Utilización de interfaces de red Ethernet de 10/100 Mbps

Tabla 36. Configuraciones que pueden resultar en discrepancias de las modalidades de dúplex durante el funcionamiento

Configuración		Resultado	
IBM 2216	Hub/Switch	IBM 2216	Hub/Switch
Auto	FDX*	HDX*	FDX
Auto	10	10	10
Auto	FDX	HDX	FDX
Auto	100	100	100
HDX	FDX	HDX	FDX
Auto	10	10	10
HDX	FDX	HDX	FDX
Auto	100	100	100
Auto	FDX	HDX	FDX
10	10	10	10
Auto	FDX	HDX	FDX
100	100	100	100
HDX	FDX	HDX	FDX
10	10	10	10
FDX	HDX	FDX	HDX
Auto	10	10	10
FDX	HDX	FDX	HDX
Auto	100	100	100
HDX	FDX	HDX	FDX
100	100	100	100
FDX	HDX	FDX	HDX
10	10	10	10
FDX	HDX	FDX	HDX
100	100	100	100

* HDX = Semi-dúplex FDX = Dúplex

Capítulo 22. Configuración y supervisión de la interfaz de red Ethernet de 10/100 Mbps

Este capítulo describe los mandatos de configuración y operativos de la interfaz Ethernet de 10/100 Mbps . Incluye las secciones siguientes:

- “Acceso al proceso de configuración de interfaces”
- “Mandatos de configuración de Ethernet de 10/100-Mbps”
- “Acceso al proceso de supervisión de interfaces Ethernet” en la página 288
- “Mandatos de supervisión de la interfaz Ethernet de 10/100 Mbps” en la página 289
- “Soporte para la reconfiguración dinámica de Ethernet” en la página 289

Acceso al proceso de configuración de interfaces

Utilice el procedimiento siguiente para acceder al proceso de configuración. Este proceso le proporciona acceso al proceso de *configuración* de una interfaz Ethernet.

1. En el indicador OPCON, entre **configuration**. (Para ver los detalles de este mandato, consulte la sección “¿Qué es el proceso OPCON?” en la página 33.)
Por ejemplo:

```
* configuration
Config>
```

Se visualiza el indicador CONFIG (Config>) en la consola. Si no aparece el indicador cuando entre en la configuración, pulse **intro** de nuevo.

2. En el indicador CONFIG, entre el mandato **list devices** para visualizar los números de interfaces para las que el dispositivo está configurado actualmente.
3. Anote los números de interfaz.
4. Entre el mandato **network** y el número de la interfaz Ethernet que desea configurar. Por ejemplo:

```
Config> network 0
Ethernet interface configuration
ETH Config>
```

Se visualiza el indicador de configuración Ethernet (ETH Config>).

Mandatos de configuración de Ethernet de 10/100-Mbps

Esta sección describe los mandatos de configuración Ethernet de 10/100-Mbps . Entre los mandatos en el indicador ETH config>.

Tabla 37. Resumen de los mandatos de configuración de Ethernet

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página 10.
Duplex	Establece la modalidad de dúplex. (Sólo para Ethernet de 10/100 Mbps.)
IP-Encapsulation	Establece la encapsulación IP como Ethernet (tipo X'0800'), IEEE (802.3 con SNAP) o ambos.
List	Visualiza el tipo de conector y la encapsulación IP actuales.
Physical-Address	Establece la dirección MAC física.

Configuración de interfaces de red Ethernet

Tabla 37. Resumen de los mandatos de configuración de Ethernet (continuación)

Mandato	Función
Speed	Establece la velocidad de enlace.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página 11.

Duplex

Utilice el mandato **duplex** para establecer la modalidad de dúplex. Este mandato sólo es para Ethernet de 10/100 Mbps.

Nota: Se recomienda el valor por omisión *auto*. Sólo deben especificarse los valores **half-duplex** o **full-duplex** si la negociación automática no da como resultado la activación satisfactoria de la interfaz o de la modalidad de dúplex deseada. Observe en la sintaxis del mandato que para semi-dúplex o dúplex se escribe con un subrayado entre las palabras, por ejemplo, *half_duplex*.

Si se especifica un valor distinto a *auto*, asegúrese de que el mismo valor está configurado en el puerto del conmutador. Después de configurar el puerto del conmutador para que coincida con el dúplex especificado en la interfaz Ethernet de 10/100 Mbps, inhabilite y pruebe la interfaz.

Verifique que la modalidad de dúplex real que aparece en el panel de estado de la interfaz coincide con el valor operativo del puerto del conmutador.

La interfaz puede entrar en estado activado con una discrepancia en la modalidad de dúplex. El funcionamiento con discrepancia de las modalidades de dúplex en la interfaz y en el puerto del conmutador puede ocasionar una grave degradación del rendimiento.

Consulte la sección “Configuración de valores distintos de automático para dúplex” en la página 281 para obtener información acerca de la modalidad de dúplex.

Sintaxis:

```
duplex          _half_duplex
                _full_duplex
                _auto
```

Half_duplex

La interfaz no transmitirá mientras reciba ni recibirá mientras transmita.

Full_duplex

La interfaz transmitirá y recibirá simultáneamente.

Auto La interfaz seleccionará automáticamente semi-dúplex o dúplex dependiendo de la posibilidad del asociado del enlace.

IP-Encapsulation

Utilice el mandato **IP-encapsulation** para seleccionar Ethernet (Ethernet tipo X'0800'), IEEE 802.3 (Ethernet 802.3 con SNAP) o ambos. El valor por omisión es Ethernet.

Configuración de interfaces de red Ethernet

La opción **both** permite que el 2216 utilice la encapsulación Ethernet para transmitir a los sistemas principales que tienen encapsulación Ethernet y utilizar la encapsulación IEEE 802.3 para transmitir a los sistemas principales que tienen encapsulación IEEE 802.3. Si la LAN Ethernet incluye unos sistemas principales que utilizan un tipo de encapsulación y otros que utilizan el otro, si se entra **both** permite que todos ellos se comuniquen.

La opción **both** sólo se aplica a las tramas de vertimiento único. Si entra **both**, se le solicita que entre **ethernet** o **ieee-802.3** para las tramas de difusión o de multidifusión.

Sintaxis:

IP-encapsulation

- ethernet
- ieee-802.3
- both

Ejemplo:

```
Eth Config [1]>ip-encapsulation both
How would you like IP broadcast/multicast frames to be sent (ETHER/IEEE-802.3) [ETHER]?
```

List

Utilice el mandato **list** para visualizar la configuración actual para la interfaz Ethernet de 10/100 Mbps .

Sintaxis:

list all

Ejemplo:

```
list all
Eth Config [2]>list all
Connector type:      RJ45 (10BASET)
IP Encapsulation:   ETHER
MAC Address:        023456789A56
```

Physical-Address

Utilice el mandato **physical-address** para establecer la dirección física (MAC).

Sintaxis:

physical-address address

physical-address

Este mandato le permite indicar si desea definir una dirección administrada localmente para la dirección de subcapa MAC de la interfaz Ethernet o utilizar la dirección por omisión incorporada (indicada por sólo ceros). La dirección de subcapa MAC es la dirección que la interfaz Ethernet utiliza para recibir y transmitir tramas.

Nota: Si se pulsa **Intro** el valor se deja igual. Si se entra **0** hace que el dispositivo utilice la dirección incorporada. El valor por omisión es utilizar la dirección incorporada.

Valores válidos: Cualquier dirección hexadecimal de 12 dígitos.

Valor por omisión: dirección incorporada (indicada por sólo ceros).

Configuración de interfaces de red Ethernet

Ejemplo:

```
physical-address  
MAC address in 00:00:00:00:00:00 form []? 12:15:00:FA:00:FE
```

Speed

Utilice el mandato **speed** para establecer la velocidad utilizada por esta interfaz.

Nota: Se recomienda el valor por omisión *automática* para la Ethernet de 10/100 Mbps. Los valores **ten** y **hundred** sólo deben especificarse si la negociación automática no da como resultado la activación satisfactoria de la interfaz o la velocidad deseada.

Si se especifica un valor distinto a *auto*, asegúrese de que el mismo valor está configurado en el puerto del conmutador. Después de configurar el puerto del conmutador para que coincida con la velocidad especificada en la interfaz Ethernet de 10/100 Mbps, inhabilite y pruebe la interfaz.

Si la interfaz y el puerto de conmutador (o concentrador) no están configurados para una velocidad idéntica, la interfaz no conseguirá el estado activado.

Consulte la sección “Negociación automática en la interfaz Ethernet de 10/100 Mbps” en la página 281 para obtener información sobre la negociación automática.

Sintaxis:

```
speed                ten  
                       hundred  
                       auto
```

Ten La interfaz de 10/100 Mbps funcionará a 10 Mbps.

Hundred

La interfaz de 10/100 Mbps funcionará a 100 Mbps

Auto La interfaz de 10/100 Mbps seleccionará automáticamente la velocidad (10 Mbps o 100 Mbps) dependiendo de la posibilidad del asociado en el enlace.

Acceso al proceso de supervisión de interfaces Ethernet

Para supervisar la información relacionada con la interfaz de red Ethernet de 10/100 Mbps, acceda al proceso de supervisión de interfaces efectuando lo siguiente:

1. En el indicador OPCON, entre **console**. Por ejemplo:

```
* console
```

Se visualiza el indicador GWCON (+) en la consola. Si no aparece el indicador cuando entre en GWCON, pulse **intro** de nuevo.

2. En el indicador GWCON, entre el mandato **configuration** para ver los protocolos y las redes para los que está configurado el dispositivo. Por ejemplo:

```
+ configuration
```

Consulte la sección “Configuration” en la página 120 para ver un ejemplo de salida del mandato **configuration**.

Configuración de interfaces de red Ethernet

- Entre el mandato **network** y el número de interfaz Ethernet, tal como se muestra en el ejemplo siguiente:

```
+ network 0
ETH>
```

Se visualiza el indicador de supervisión Ethernet. Ahora, puede ver la información acerca de la interfaz Ethernet entrando los mandatos de supervisión.

Mandatos de supervisión de la interfaz Ethernet de 10/100 Mbps

Esta sección resume los mandatos de supervisión Ethernet de 10/100 Mbps . Entre los mandatos en el indicador ETH>.

Tabla 38. Resumen de los mandatos de supervisión Ethernet

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página 10.
Collisions	Visualiza las estadísticas de colisión para la interfaz Ethernet especificada.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página 11.

Collisions

Este mandato visualiza las cuentas de las transmisiones de paquetes que han incurrido en colisiones antes de la transmisión satisfactoria. Se visualizan contadores para los paquetes enviados después de 15 colisiones. El aumento del número de paquetes transmitidos con colisiones y números altos de colisiones por paquete son signos de una transmisión en una Ethernet ocupada.

El mandato **CLEAR** de OPCON borra estos contadores. Estos datos se exportan mediante SNMP como el contador dot3CollTable.

Sintaxis:

collisions

Ejemplo:

```
Eth> coll
Transmitted with 1 collisions:0
Transmitted with 2 collisions:0
Transmitted with 3 collisions:0
Transmitted with 4 collisions:0
Transmitted with 5 collisions:0
Transmitted with 6 collisions:0
Transmitted with 7 collisions:0
Transmitted with 8 collisions:0
Transmitted with 9 collisions:0
Transmitted with 10 collisions:0
Transmitted with 11 collisions:0
Transmitted with 12 collisions:0
Transmitted with 13 collisions:0
Transmitted with 14 collisions:0
Transmitted with 15 collisions:0
```

Soporte para la reconfiguración dinámica de Ethernet

Esta sección describe la reconfiguración dinámica (DR) en la medida en que afecta a los mandatos Talk 6 y Talk 5.

Configuración de interfaces de red Ethernet

Delete Interface de CONFIG (Talk 6)

Ethernet soporta el mandato **delete interface** de CONFIG (Talk 6) sin ninguna restricción.

Activate Interface de GWCON (Talk 5)

Ethernet soporta el mandato **activate interface** de GWCON (Talk 5) sin ninguna restricción.

El mandato **activate interface** de GWCON (Talk 5) soporta todos los mandatos específicos de interfaz Ethernet.

Reset Interface de GWCON (Talk 5)

Ethernet soporta el mandato **reset interface** de GWCON (Talk 5) sin ninguna restricción.

El mandato **reset interface** de GWCON (Talk 5) soporta todos los mandatos específicos de interfaz Ethernet.

Capítulo 23. Visión general de LAN Emulation

Nota: Consulte el glosario para ver las definiciones de los acrónimos y los términos utilizados en este capítulo.

El IBM 2216 implementa la *Especificación LAN Emulation a través de ATM: Versión 1.0* que está ampliamente aceptada como el estándar de la industria para la interoperatividad de protocolos de múltiples proveedores. Este capítulo introduce los conceptos básicos de LAN Emulation (LE) en el contexto de la implementación de IBM 2216. Empieza por el examen de los motivos para instalar las LAN emuladas (ELAN).

Beneficios de LAN Emulation

Los protocolos de la emulación de LAN permiten que las redes ATM proporcionen la apariencia de LAN Ethernet y Red en Anillo. Aunque la emulación de LAN no explota todos los beneficios de ATM, es útil en la migración a la tecnología ATM y reduce los costes de gestión de la red. Le permite utilizar enlaces ATM de alta velocidad y seguir protegiendo las inversiones de hardware y de software.

Las inversiones en software están protegidas porque las interfaces de aplicación no cambian (LAN Emulation se implementa en la capa de control de enlace de datos, que está por debajo de la interfaz del controlador de dispositivos de las estaciones finales). Las inversiones en hardware están protegidas por máquinas de reenvío que puentean las redes LAN y ATM para que se pueda continuar utilizando los adaptadores y el cableado existente.

LAN Emulation permite una instalación por fases de los adaptadores ATM en las estaciones con requisitos de ancho de banda superior, por ejemplo, los servidores y el servicio técnico o las estaciones de trabajo multimedia. Las vistas física y lógica de un ejemplo sencillo de LAN Emulation se ilustran en la Figura Figura 15 en la página 292.

Visión general de LAN Emulation

Red sencilla de LAN Emulation

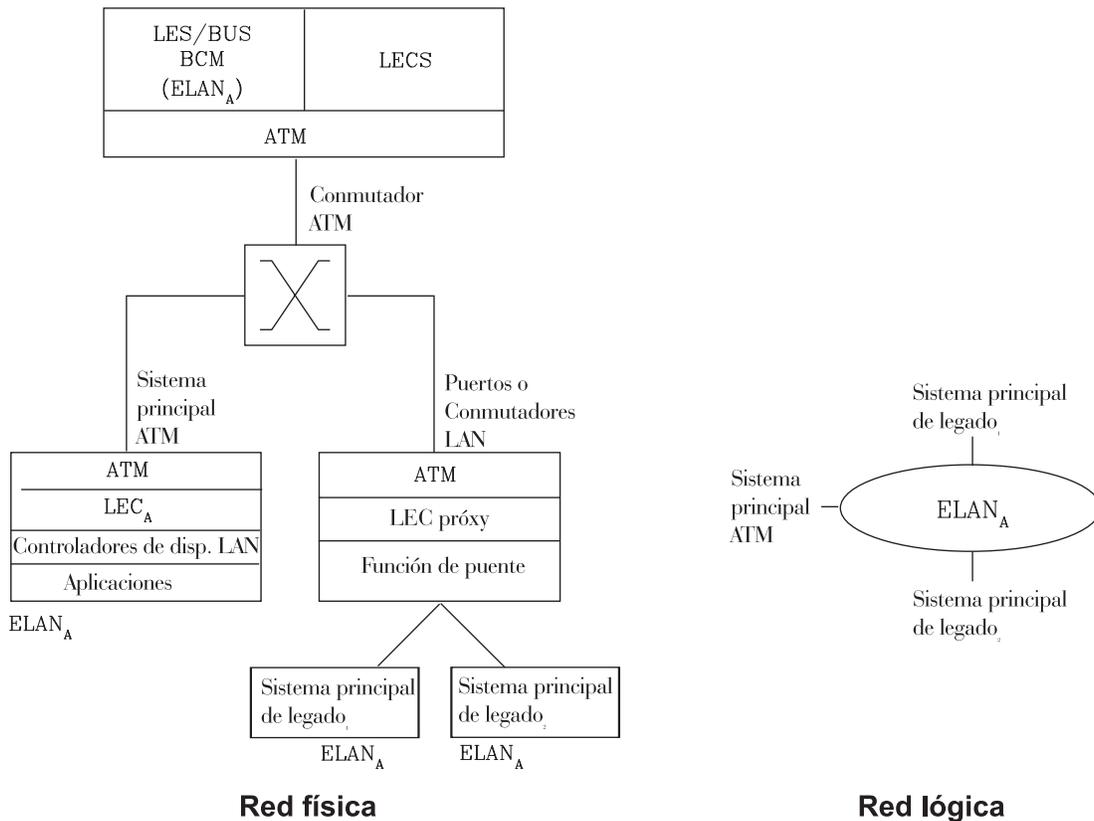


Figura 15. Vistas física y lógica de una red sencilla de LAN Emulation

Los beneficios de la gestión de redes de las LAN emuladas (ELAN) aumentan por una flexibilidad incrementada en el manejo de traslados, adiciones y cambios. La pertenencia a una ELAN no se basa en la ubicación física; en su lugar, las estaciones relacionadas lógicamente se agrupan formando una ELAN (las estaciones también pueden ser miembros de múltiples ELAN).

Mientras se conserven los miembros de las ELAN, no será necesaria ninguna reconfiguración cuando las estaciones se trasladen a nuevas ubicaciones físicas. De manera similar, no es necesaria ninguna modificación del cableado para trasladar estaciones de una ELAN a otra.

Componentes de LAN Emulation

Los componentes siguientes implementan una ELAN:

LAN Emulation (LE) clients (LEC)

Los componentes de LAN Emulation que representan a los usuarios de la LAN emulada.

LE configuration server (LECS)

Un componente de servicio de LAN Emulation que centraliza y disemina los datos de configuración.

LE server (LES)

Un componente del servicio de LAN Emulation que resuelve los destinos de LAN en las direcciones ATM.

Broadcast and Unknown Server (BUS)

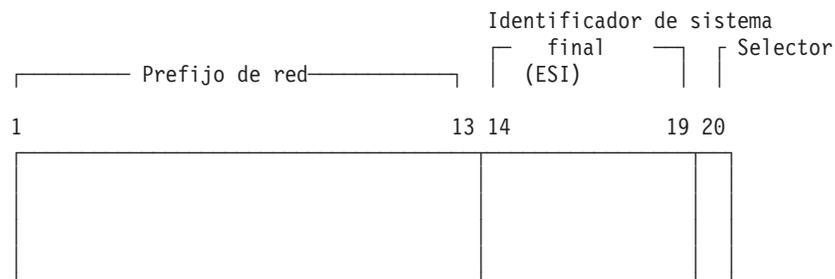
Un componente del servicio de LAN Emulation responsable de la entrega de tramas de multidifusión y de vertimiento único desconocidas.

Se hace referencia a LES, BUS y LECS colectivamente como los componentes del servicio LE. Cada ELAN tiene LES y BUS dedicados. Los clientes LE residen en sistemas finales, ya sean sistemas principales conectados a ATM o puentes o conmutadores LAN. Los puentes o conmutadores LAN representan sistemas principales que se conectan a las LAN Ethernet o de Red en Anillo. Los clientes LE proporcionan un servicio a nivel MAC para el software de nivel superior. Se pueden emular LAN Ethernet IEEE 802.3 o de Red en Anillo IEEE 802.5, pero todas las estaciones de una ELAN deben ser del mismo tipo.

La función que sirve de puente entre los segmentos de LAN de Red en Anillo y Ethernet y las ELAN se llama un LEC Proxy. Para emular una LAN, los clientes LE piden los servicios de LECS, LES y BUS. Las secciones siguientes revisan brevemente el direccionamiento ATM y las funciones pertinentes de Interim Local Management Interface (ILMI). Es necesario que comprenda estos conceptos para poder entender cómo funcionan los componentes LE en la red.

Direccionamiento en ATM

ATM utiliza un direccionamiento jerárquico de 20 bytes:



Los 13 primeros octetos de una dirección ATM son el Prefijo de red. Cada conmutador de la red ATM debe tener un Prefijo de red exclusivo. Los conmutadores ATM utilizan el Prefijo de red para direccionar las peticiones configuradas de VCC al conmutador ATM de destino. Los sistemas finales, como este direccionador, recuperan su Prefijo de red del conmutador ATM cuando se activan.

Los octetos 14–19 de una dirección ATM son el Identificador del sistema final (ESI). Cada sistema final conectado al mismo conmutador debe utilizar un conjunto inconexo de ESI. Cuando se activa un sistema final, intenta registrar sus ESI en su conmutador ATM utilizando la Interim Local Management Interface (ILMI).

La ILMI define un conjunto de procedimientos basados en SNMP que se utilizan para gestionar la interfaz entre un sistema final y un conmutador ATM. Los sistemas finales utilizan ILMI para:

- Obtener el prefijo de red del conmutador
- Registrar sus ESI en el conmutador
- Determinar dinámicamente la versión UNI del conmutador ATM
- Los LEC pueden obtener una lista de direcciones LECS del conmutador

Visión general de LAN Emulation

El conmutador obliga a que todos sus ESI registrados sean exclusivos.

El octeto 20 de una dirección ATM es el selector.

Las estaciones finales obtienen su Prefijo de red del conmutador y forman sus propias direcciones añadiendo un ESI y el selector. Estas direcciones deben registrarse en el conmutador, que rechaza el registro si la dirección ATM no es exclusiva.

ESI

Cada interfaz ATM del direccionador tiene una dirección MAC administrada universalmente o incorporada. Puede utilizar la dirección MAC como ESI para algunas o todas las direcciones ATM del direccionador. Alternativamente, puede definir hasta 64 ESI administrados localmente en cada interfaz. Si cada sistema final utiliza su dirección MAC administrada universalmente como su ESI, se garantiza que las direcciones ATM son exclusivas. Esto facilita el trabajo de configuración. Sin embargo, la utilización de ESI administrados localmente puede facilitar la determinación de problemas. Puede utilizar cualquier combinación de ESI administrados universal o localmente.

Una manera de obtener una dirección ATM exclusiva es utilizar la dirección MAC IEEE incorporada como el ESI y elegir localmente un selector exclusivo. Por omisión, el direccionador utiliza la dirección MAC de la interfaz ATM como ESI en sus direcciones ATM. Se pueden configurar ESI adicionales en cada interfaz ATM.

Cada ESI puede tener hasta 255 selectores asociados (de 0x00 a 0xff). El rango de selectores se divide en dos subrangos, un rango de selectores configurados y un rango de selectores asignados automáticamente. El parámetro de la interfaz ATM max-configured-selector proporciona el límite superior del rango de selectores configurados.

Los componentes ATM del direccionador tienen varias maneras de elegir un selector. Algunos componentes necesitan que el usuario configure explícitamente un selector del rango de selectores configurados. LES/BUS son ejemplos de dichos componentes. Otros componentes, por ejemplo, los clientes Classical IP permiten que se asigne el selector automáticamente en el momento de la ejecución. No tiene que elegir el selector porque el direccionador lo hace cuando se activa. No se garantiza la coherencia de este selector en los reinicios del direccionador. La asignación automática del selector sólo es útil para los componentes ATM cuya dirección ATM no tiene que ser conocida aún por otros dispositivos de la red.

Debe configurar ATM antes de configurar las LAN emuladas, el puente o el direccionamiento.

Direcciones ATM de componentes de LAN Emulation

En general, las direcciones ATM deben ser exclusivas entre los componentes de LAN Emulation. La única excepción es que un LES y BUS que sirven la misma ELAN pueden compartir una dirección ATM, como es el caso del direccionador.

Los componentes de LAN Emulation están configurados para una interfaz ATM en particular. Puede decidir utilizar la dirección MAC incorporada como la parte ESI de la dirección ATM del componente o puede seleccionar uno de los ESI administrados localmente que se han definido para la interfaz ATM. Varios componentes LE pueden compartir el mismo ESI si tienen selectores exclusivos.

Visión general de LAN Emulation

Por omisión, la interfaz de configuración asigna a cada componente LE un valor de selector exclusivo para el ESI configurado; sin embargo, puede alterar temporalmente esta asignación y configurar explícitamente un valor de selector en particular.

Un parámetro de la interfaz ATM determina el número de selectores por ESI reservados para la asignación explícita. El resto están disponibles para que la interfaz ATM los asigne dinámicamente en tiempo de ejecución. Los componentes LE sólo utilizan los selectores reservados para la asignación explícita; por omisión, 200 de los 256 posibles selectores por ESI están reservados para la asignación explícita. La asignación del selector en tiempo de ejecución es beneficiosa cuando no se necesita controlar el selector asignado, por ejemplo, cuando se configuran clientes en Classical IP que no están emparejados con un servidor ARP.

Mientras las direcciones ATM deben ser exclusivas entre los componentes LE, éstos pueden utilizar las mismas direcciones ATM que los componentes que no son LE, por ejemplo servidores Classical IP.

Visión general de las funciones de ILMI relacionadas

ILMI define un conjunto de procedimientos basados en SNMP que se utilizan para gestionar la interfaz de red del usuario (UNI) entre un sistema final ATM y un conmutador ATM. Las tres funciones ILMI siguientes son especialmente importantes para LAN Emulation:

1. El registro de direcciones ATM, que se describe en la sección “Direccionamiento en ATM” en la página 293
2. La determinación dinámica de la versión de señalización que se ejecuta en el conmutador
3. La adquisición de direcciones ATM del LECS

Tal como se menciona en la sección “Direccionamiento en ATM” en la página 293, el registro de direcciones ATM es un esfuerzo común entre sistemas finales ATM y conmutadores. Las direcciones ATM deben registrarse en el conmutador antes de que se puedan realizar o recibir llamadas.

Por omisión, las interfaces ATM de un direccionador utilizan procedimientos ILMI para consultar la MIB del conmutador para intentar determinar la versión de la señalización (UNI 3.0 ó 3.1) que se ejecuta en el conmutador. Si la consulta es satisfactoria, la interfaz ATM ejecuta la misma versión de UNI que el conmutador; si la consulta falla, la interfaz ATM ejecuta UNI 3.0. Alternativamente, puede alterar temporalmente el valor por omisión y configurar explícitamente la versión de UNI que se ejecutará en la interfaz ATM.

Configuración manual de la versión de señalización

Es necesario configurar la versión de señalización manualmente si el conmutador ATM ejecuta UNI 3.1 y no tiene ninguna variable MIB de versión UNI. En este caso, la interfaz ATM no puede determinar dinámicamente la versión de UNI. Puesto que la interfaz ATM del direccionador utiliza UNI 3.0 por omisión, debe configurar manualmente la interfaz ATM para que utilice UNI 3.1.

Localización de LECS utilizando ILMI

ILMI es el método de elección para localizar el LECS. La ILMI de MIB del conmutador ATM incluye una lista de direcciones ATM del LECS que los clientes LE pueden recuperar. Este método es útil porque las direcciones ATM del LECS sólo necesitan configurarse en los conmutadores ATM, no en los clientes LE, y hay

Visión general de LAN Emulation

menos conmutadores que clientes LE. Los clientes intentan conectarse con el primer LECS de esta lista. Si falla la conexión, intentan la siguiente dirección LECS y así sucesivamente hasta que se establece una conexión.

Visión general de la función LECS

Los clientes LE no necesitan utilizar el LECS, aunque es aconsejable. Si no se utiliza el LECS, cada cliente LE debe estar configurado con la dirección ATM del LES que sirve su ELAN. El LECS reduce el trabajo de gestión de la red sirviendo como depósito centralizado para los datos de configuración, minimizando la configuración de los clientes LE.

Nota: Como máximo, sólo un LECS es configurable en cada direccionador.

Los clientes se conectan al LECS utilizando procedimientos bien definidos. Los pasos siguientes son los que sigue un cliente, por orden, hasta establecer una conexión de canal virtual (VCC) con el LECS:

1. Conéctese al LECS utilizando cualquier información de dirección LECS configurada (la configuración de una dirección ATM del LECS en los clientes LE es opcional y **no** se recomienda).
2. Obtenga una lista de direcciones LECS utilizando ILMI e intente conectarse a cada LECS de la lista, por orden, hasta que se establezca una VCC.
3. Establezca una VCC con la dirección ATM del LECS conocida, tal como la define el Forum ATM.

Tal como se indicaba anteriormente, ILMI es el método preferido para que los clientes LE localicen el LECS. La dirección LECS conocida es necesaria porque algunos conmutadores no soportan el método ILMI. La configuración de la dirección LECS en los clientes LE **sólo** debe realizarse cuando el conmutador no soporte el método ILMI y el servicio LE no soporte la dirección LECS conocida.

El direccionador y el conmutador IBM ATM soportan los tres métodos: la dirección del LECS preconfigurada, la conexión ILMI y la dirección del LECS conocida.

El LECS debe proporcionar datos de configuración inicial a los clientes LE. La parte más importante de los datos es la dirección ATM del LES. Para proporcionar esta información a un cliente LE, el LECS debe poder identificar el cliente LE y determinar el LES correcto para ese cliente LE. El LECS identifica un cliente LE utilizando la información de la trama LE_CONFIGURATION_REQUEST enviada por el cliente LE. La petición de configuración también puede contener información para identificar la ELAN que el cliente está buscando para unirse a ella. Puede incluirse la información siguiente en la petición de configuración:

1. La dirección ATM primaria del cliente LE
Este campo es necesario y solamente identifica al cliente LE.
2. El destino LAN asociado con el cliente LE
Este campo puede contener una dirección MAC o un descriptor de ruta que identifique exclusivamente al cliente LE o puede estar sin especificar.
3. Nombre de ELAN
Este campo puede contener un nombre que identifique la ELAN o el cliente LE que efectúa la petición. En la implementación del direccionador, los nombres de ELAN son series ASCII estándar. El nombre de ELAN puede estar sin especificar en la petición.
4. Tipo de ELAN

Visión general de LAN Emulation

Este campo puede especificar que el cliente LE pertenece a una ELAN Ethernet o Red en Anillo o puede estar sin especificar. Si el cliente LE especifica el tipo de ELAN, el LECS no puede asignar el cliente a una ELAN de tipo diferente.

5. Tamaño máximo de trama soportado por el cliente LE

Este campo puede especificar el límite superior del tamaño de una trama de datos que el cliente LE puede procesar o puede estar sin especificar. El LECS no puede asignar un cliente a una ELAN con un tamaño máximo de trama **mayor** que el especificado por el cliente. Si la ELAN permite tramas demasiado grandes para que el cliente las maneje, el cliente no puede funcionar en esa ELAN.

Después de proporcionar esta información, el LECS asigna el cliente LE a un LES. Esto se hace mediante la utilización de políticas o valores de políticas. Una política es un criterio que el LECS utiliza para tomar decisiones de asignación de cliente LE a LES. Un valor de política es un par (valor, LES) que indica que el valor especificado debe asignarse al LES especificado. Por ejemplo, una política podría ser una dirección MAC del cliente LE y un valor de política podría ser (MAC ADDR_A, LES_1). Un cliente LE con MAC ADDR_A se asignará al LES_1 si el cliente LE no se ha asignado aún a otro LES debido a una política de prioridad más alta. Se aplica un conjunto de políticas y valores de políticas a todas las ELAN.

De acuerdo a la Especificación MIB del servicio LE del forum ATM estas son las seis políticas definidas:

1. Dirección ATM
2. Dirección ATM
3. Descriptor de rutas
4. Tipo de ELAN
5. Tamaño máximo de trama
6. Nombre de ELAN

Las políticas también tienen prioridades. El LECS examina las políticas por orden de prioridad. Las políticas con valores inferiores en el campo de prioridad se toman en consideración antes que las políticas con valores superiores en el campo prioridad. Las políticas con valores iguales en el campo de prioridad se toman en consideración simultáneamente y se ejecuta *AND* para las dos.

El LECS asigna un cliente LE a un LES cuando se satisfacen todas las políticas del nivel de prioridad actual y están de acuerdo. Las políticas se satisfacen cuando hay un valor de política que coincide con el campo correspondiente de la petición de configuración para cada política del nivel actual. Las políticas están de acuerdo cuando el conjunto de coincidencias incluye un LES que es común a todas las políticas. Si no se satisfacen estas condiciones, el LECS considera las políticas del siguiente nivel de prioridad. Si el LECS no puede encontrar un LES en ningún nivel de prioridad, se devuelve una respuesta de configuración no satisfactoria al cliente LE.

Para comprender el significado del acuerdo de las políticas, considere este ejemplo de políticas que no están de acuerdo. Suponga que las políticas de la prioridad 1 son una dirección MAC y un nombre de ELAN. Uno de los valores es (X'400000121225', LES_A) y el otro es (ELAN 1, LES_B). Si el cliente LE proporciona un destino LAN de X'400000121225', se satisface la política de dirección MAC. Si el cliente LE proporciona el nombre de ELAN *ELAN 1*, la política de nombre de ELAN también se satisface. En este caso las políticas de la prioridad

Visión general de LAN Emulation

ELAN *Contabilidad*, mientras que los que pertenecen al Departamento técnico podrían utilizar el nombre de ELAN *Técnicos*. Dependiendo del número de clientes LE de las ELAN, estos nombres podrían direccionarse a la misma ELAN configurando estos valores de política:

(Contabilidad, LES_A)
(Técnicos, LES_A)

o a ELAN diferentes configurando estos valores de política:

(Contabilidad, LES_A)
(Técnicos, LES_B)

Para esta configuración es necesario configurar los clientes LE con el Nombre de ELAN correcto.

- Utilización de nombres para los clientes LE

Puede otorgarse a cada cliente LE su propio nombre. Por ejemplo, podría crear los valores de política (José, LES_A) y (María, LES_A). Después, los clientes LE configurados con estos nombres se direccionarían al mismo LES. Este método necesita la configuración del nombre de ELAN en cada cliente LE y en el LECS. Sin embargo, permite que José y María trasladen el cliente a una nueva ubicación. Aunque el traslado hace que el cliente tenga una nueva dirección ATM o dirección MAC, siempre que configure el nuevo cliente LE con el mismo nombre de ELAN, seguirá siendo miembro de la ELAN original. Esta técnica ofrece también un nivel seguridad moderado si los nombres de cada cliente LE se consideran contraseñas.

Política de tipo de ELAN

Los valores de política de tipo de ELAN son los más útiles para proporcionar las ELAN por omisión. Por ejemplo, los valores de política siguientes asegurarían que cada cliente LE se asignase a uno de los LES:

(Token-ring ELAN Type, LES_A)
(Ethernet ELAN Type, LES_B)
(Unspecified ELAN Type, LES_C)

En general, se debe otorgar una prioridad inferior a las políticas utilizadas para proporcionar asignaciones ELAN por omisión, para que las políticas más específicas se tomen en consideración primero.

Política de tamaño máximo de trama

La política de tamaño máximo de trama se utiliza para proporcionar asignaciones de ELAN por omisión.

Valores de política de duplicados

Los duplicados se producen cuando el mismo valor de política se asocia con múltiples LES para una política determinada. Los valores de política de duplicados están permitidos para las políticas de tipo de ELAN y de tamaño máximo de trama, pero no están permitidos para otras políticas. Los valores duplicados sólo son útiles cuando se combinan con una política diferente de la misma prioridad.

Por ejemplo, suponga que hay tres ELAN: una ELAN Ethernet con un tamaño máximo de trama de 4544 bytes, una ELAN de Red en Anillo con un tamaño máximo de trama de 4544 bytes y otra ELAN de Red en Anillo con un tamaño máximo de trama de 18190 bytes. Se podrían asignar los clientes LE a la ELAN adecuada estableciendo las políticas de tipo de ELAN y de tamaño máximo de trama en el mismo nivel de prioridad y definiendo los valores de política siguientes:

(Ethernet ELAN Type, LES_1) (Max Frame Size = 4544, LES_1)
(Token-Ring ELAN Type, LES_2) (Max Frame Size = 4544, LES_2)
(Token-Ring ELAN Type, LES_2) (Max Frame Size = 18190, LES_2)

Visión general de LAN Emulation

Más información acerca de los parámetros TLV

Los parámetros TLV se definen por ELAN; por lo tanto, se devuelve el mismo conjunto de TLV a todos los clientes LE que se asignan a una ELAN en particular. Cuando se incluye un TLV en una respuesta de configuración, el cliente LE **debe** utilizar el valor especificado en el TLV como parámetro operativo (si el cliente LE reconoce el tipo de ELAN). Los siguientes ejemplos son situaciones en las que los TLV pueden ser beneficiosos:

- Cuando las ELAN están esparcidas en ubicaciones geográficas grandes, los valores de tiempo de espera excedido por omisión para los clientes LE pueden ser insuficientes. Estos tiempos de espera excedidos pueden controlarse para todos los clientes LE especificando su valor en un TLV en el LECS.
- Por omisión, las ELAN utilizan conexiones de mejor esfuerzo para conectarse al BUS. Para las ELAN en que el tráfico de BUS es grande, se puede obtener un mejor rendimiento utilizando las conexiones de ancho de banda reservado para el BUS. Las características de la VCC de envío de multidifusión entre el cliente LE y el BUS puede controlarse con los TLV.
- Se puede utilizar un TLV para descargar el número de segmento de ELAN en los puentes de ruta de origen.

Además de ajustar con precisión la configuración, los TLV fuerzan a todos los clientes de la ELAN a funcionar con parámetros coherentes. El IBM 2216 soporta todos los TLV definidos en el Forum ATM junto con los TLV arbitrarios, definidos por el usuario.

Conexión al LES

Después de obtener la dirección ATM del LES, el cliente LE inicia una VCC de control directo con el LES. Cuando se ha establecido esta VCC, el cliente LE envía una petición LE_JOIN_REQUEST al LES. El LES responde añadiendo el cliente LE a la VCC adecuada de distribución de control de punto a multipunto y devolviendo una respuesta LE_JOIN_RESPONSE. Por omisión, el LES divide a los clientes proxy y no proxy en VCC de control de distribución separadas, tal como se ilustra en la Figura 16 en la página 301; sin embargo, puede configurar el LES para que todos los clientes LES utilicen una sola VCC de control de distribución para reducir el número de VCC de punto a multipunto que son necesarias. Generalmente, la partición de VCC es útil porque reduce la cantidad molesta de tráfico que se envía a clientes no proxy. No se envían peticiones LE_ARP_REQUEST a clientes LE no proxy, tal como se describe en la sección “Resolución de direcciones” en la página 301.

Visión general de LAN Emulation

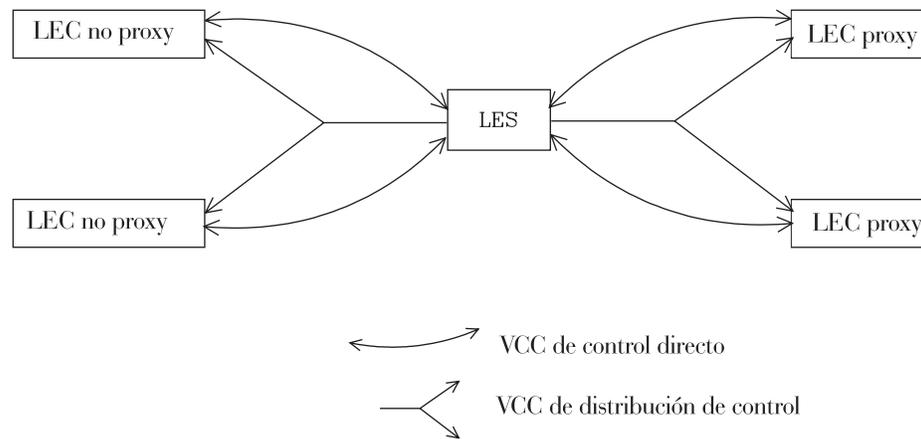


Figura 16. Conexiones por omisión entre clientes LE Client y el LES

Las conexiones ATM siguientes se establecen entre el cliente LE y el LES:

VCC de control directo (bidireccional punto a punto)

Desde el cliente LE al LES

VCC de control de distribución (punto a multipunto)

Desde el LES al cliente LE

Registro de direcciones

Los clientes LE registran los destinos LAN en el LES para asegurar la exclusividad y para permitir al LES responder a la petición LE_ARP_REQUEST, que los clientes LE emiten para conocer la dirección ATM asociada con un destino LAN en particular. Los registros incluyen el destino LAN y la dirección ATM que el cliente LE asocia con el destino LAN. Un destino LAN puede ser una dirección MAC o un descriptor de ruta.

Los clientes LE proxy no registran las direcciones MAC de estaciones de los segmentos de la LAN que puentean hasta la ELAN. Por otro lado, los clientes LE no proxy deben registrar todos los destinos LAN que representan. Todos los descriptors de rutas deben estar registrados, sin tener en cuenta si están asociados con un cliente LE proxy o no proxy. Los descriptors de rutas sólo se pueden aplicar a los LEC proxy que efectúan un puente de ruta de origen. Un descriptor de ruta contiene el número de puente del cliente LE proxy y el número de segmento de un anillo al que el cliente LE puentea que es equivalente a un salto más.

Resolución de direcciones

Las comunicaciones LAN se basan en direcciones MAC de origen y de destino. Para habilitar esta comunicación en una red ATM, deben resolverse las direcciones MAC en direcciones ATM. Un cliente LE envía una petición LE_ARP_REQUEST al LES para conocer la dirección ATM de un destino LAN en particular. Si el destino LAN está registrado, el LES responde con una dirección ATM asociada con el destino LAN. De lo contrario, la petición se reenvía a todos los clientes LE proxy de la VCC de distribución de control. No hay necesidad de reenviar la petición a los LEC no proxy porque todos sus destinos LAN están registrados; sin embargo, si el LES está configurado para utilizar una sola VCC de distribución de control,

Visión general de LAN Emulation

recibirán la petición los clientes proxy y no proxy. Las VCC de distribución de control proporcionan una forma eficaz para que el LES distribuya las tramas de control a múltiples clientes LE.

Los clientes LE proxy responden a las peticiones LE_ARP_REQUEST de las direcciones MAC no registradas que representan. La respuesta LE_ARP_RESPONSE se envía al LES de la VCC de control directo y el LES reenvía la respuesta al cliente LE que ha emitido la petición.

Conexión al BUS

Después de conectarse al LES, un cliente LE emite una petición LE_ARP_REQUEST de la dirección MAC de difusión de sólo 1. El LES responde con la dirección ATM del BUS. El cliente LE inicia el establecimiento de una VCC de envío de multidifusión al BUS. El BUS responde añadiendo el cliente LE a la VCC adecuada de reenvío de multidifusión de punto a multipunto. Por omisión, el BUS divide los clientes proxy y no proxy en VCC de reenvío de multidifusión separadas; sin embargo, igual que con la VCC de distribución de control, puede configurar el BUS para que utilice una sola VCC de reenvío de multidifusión para todos los clientes LE. La Figura 17 muestra las VCC de reenvío de multidifusión particionadas.

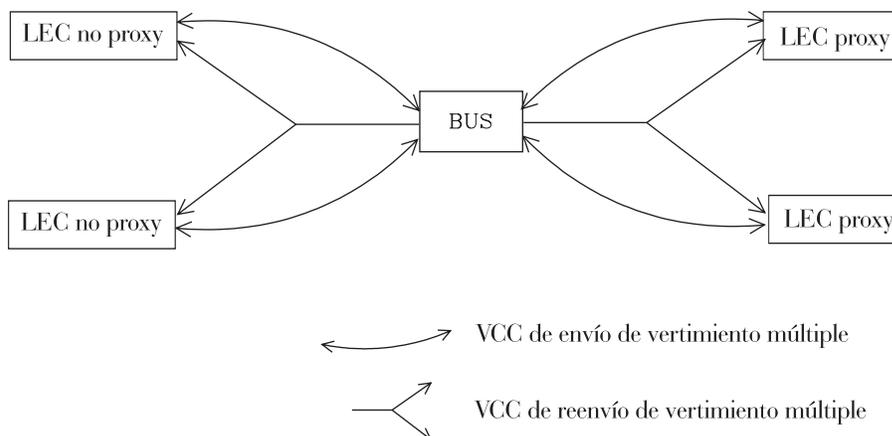


Figura 17. Conexión por omisión entre clientes LE (LEC) y el BUS

Esta lista se proporciona para ayudarle a clarificar las conexiones ATM que se establecen entre el cliente LE y el BUS:

VCC de envío de multidifusión (bidireccional de punto a multipunto)

Desde el cliente LE al BUS

VCC de reenvío de multidifusión (de punto a multipunto)

Desde el BUS al cliente LE

Funciones del BUS

El BUS tiene dos funciones básicas:

1. Distribuir tramas de multidifusión a todos los clientes LE de la ELAN
2. Reenviar tramas de vertimiento único a los destinos adecuados

Un cliente LE envía tramas de vertimiento único al BUS si no tiene una conexión directa con el cliente LE que representa el destino. Para evitar la creación de un

cuello de botella en el BUS, se limita la velocidad a la que el cliente LE puede enviar tramas de vertimiento único al BUS.

En la implementación del direccionador, el BUS tiene dos modalidades de funcionamiento: partición del dominio de tramas de vertimiento único y no partición del dominio de tramas de vertimiento único. Si particiona el dominio de tramas de vertimiento único, el BUS utiliza dos VCC de reenvío de multidifusión. De lo contrario, el BUS utiliza una sola VCC de reenvío de multidifusión.

Si se utiliza una VCC de reenvío de multidifusión, el funcionamiento del BUS es muy simple; todas las tramas recibidas se reenvían a todos los clientes LE. Si se utilizan dos VCC de reenvío de multidifusión, el BUS no difundirá las tramas de vertimiento único a todos los clientes LE; en su lugar, las tramas de vertimiento único destinadas a clientes LE no proxy se transmitirán directamente al cliente LE de destino en una VCC de envío de multidifusión y las demás tramas de vertimiento único sólo se transmitirán a clientes LE no proxy utilizando la VCC de reenvío de multidifusión proxy. Cuando se utilizan dos VCC de multidifusión, se considera que el direccionador está en modalidad de BUS inteligente (IBUS).

La modalidad IBUS reduce las tramas de vertimiento único molestas, que son tramas de vertimiento único no destinadas al cliente; los clientes proxy no reciben las tramas de vertimiento único destinadas a los clientes no proxy y los clientes no proxy no reciben nunca las tramas de vertimiento único molestas. El ancho de banda de red dedicado a las tramas molestas también se reduce. Por otro lado, los requisitos del proceso de BUS aumentan y las tramas de multidifusión deben transmitirse dos veces (una en cada VCC de reenvío de multidifusión). En general, se recomienda la utilización de IBUS; sin embargo, debe inhabilitarse esta opción en las configuraciones que tienen puentes de ruta de origen que se unen a la ELAN como no proxy.

Establecimiento de una VCC de datos directos

Las VCC de datos directos conectan dos clientes LE y se utilizan para intercambiar tramas de vertimiento único sin implicar al BUS. El cliente LE utiliza los procedimientos para la resolución de direcciones para determinar la dirección ATM asociada con el destino de LAN necesario. Si el cliente LE ya tiene una VCC de datos directos con la dirección ATM (quizás para otro destino de LAN representado por el cliente LE de destino), se transmiten las tramas de datos de vertimiento único con posterioridad en la VCC existente; de lo contrario, el cliente LE invoca el protocolo de señalización para establecer una nueva VCC.

El cliente LE mantiene una antememoria LE_ARP que contiene correlaciones de direcciones de destino LAN con ATM. Las entradas en la antememoria se quedan antiguas y deben renovarse periódicamente. Las entradas se renuevan cuando se recibe una trama de datos del destino de LAN. El cliente LE también intenta renovar las entradas en ausencia de tráfico de datos.

La utilización de las VCC de datos directos también se supervisa y las VCC se liberan si no hay tráfico durante el período de tiempo de espera excedido de la VCC, que se puede configurar. Además, las VCC de datos directos se liberan de una manera que se utiliza menos recientemente cuando falla el establecimiento de una nueva VCC de datos directos debido a la insuficiente disponibilidad de recursos.

Visión general de extensiones para LAN Emulation

IBM ha creado extensiones de valor añadido para ATM Forum LAN Emulation disponibles en el direccionador. Esta oferta de extensiones ha mejorado el rendimiento, la fiabilidad, la seguridad y la manejabilidad:

Broadcast Manager (BCM)

Esta función puede mejorar el rendimiento global de la red mediante la reducción de difusiones de la ELAN.

Redundancy

El mecanismo de redundancia mejora la fiabilidad permitiendo que los servidores de reserva tomen el control si se producen anomalías en los servidores primarios.

Security

La seguridad se mejora dejando que el LECS controle los miembros de la ELAN.

BUS Monitor

Esta función mejora la manejabilidad mediante la identificación de los principales usuarios del BUS.

Las secciones siguientes describen cada una de estas extensiones.

Broadcast Manager

Broadcast Manager (BCM) es una extensión a LAN Emulation que consiste en una mejora que IBM hace al BUS de LAN Emulation. Sin BCM, se producen los sucesos siguientes:

- Una trama de multidifusión enviada al BUS se reenvía a todos los clientes LE de la ELAN.
- Los clientes LE que incluyen la función proxy para proporcionar la función de puente soportan el reenvío de tramas de difusión a otros segmentos de la LAN.
- Todas las estaciones finales reciben y procesan cada trama de difusión.

BCM se puede habilitar en las ELAN individuales para cualquiera de estos protocolos:

IP
IPX
NetBIOS

Cuando se habilita BCM, se decodifica una cantidad mínima de información de la capa 2 y la capa 3 para tipos específicos de tramas de difusión enviadas al BUS. Siempre que es posible, BCM transforma las tramas de difusión en tramas de vertimiento único y las envía sólo a los clientes LE interesados y a las estaciones finales. BCM reduce el tráfico de red y la actividad asociada a la estación final filtrando las tramas de difusión molestas. Estas funciones pueden mejorar el rendimiento global del sistema y permitir un despliegue práctico de las ELAN mayores.

Soporte BCM para IP

Cuando se habilita para IP, BCM explora todas las peticiones y respuestas ARP de IP para conocer la ubicación de las direcciones IP en la subred IP que contiene esta ELAN. El objetivo es que BCM tome cada trama de petición ARP de difusión y la reenvíe como una trama de vertimiento único directamente al cliente LE que representa la estación IP de destino. Se reduce el tráfico de red y el tiempo de proceso de la estación final cuando la petición se reenvía directamente al cliente

LE adecuado de la VCC de envío de multidifusión en lugar de difundirse a todos los clientes LE de las VCC de reenvío de multidifusión. Cuando la estación de destino está ubicada detrás de una función de puente, la LAN a la que pertenece la estación de destino también se beneficia de la reducción del tráfico de difusión.

Soporte BCM para IPX

Para IPX, BCM limita el ámbito de anuncios y otras peticiones de difusión. Los direccionadores y servidores IPX difunden periódicamente su información conocida de red y de servicio. Los clientes IPX envían peticiones de difusión para localizar un servicio o direccionador en particular. Generalmente, sólo es necesario que reciban estas difusiones, llamadas paquetes Routing Information Protocol (RIP) y Service Advertising Protocol (SAP), otros direccionadores y servidores IPX.

Cuando está habilitado para IPX, BCM identifica dinámicamente el conjunto de direccionadores y servidores IPX basándose en las transmisiones de anuncio y sólo reenvía los anuncios RIP y SAP y otras peticiones de difusión a otros direccionadores y servidores IPX. Una trama de difusión gestionada por BCM IPX se envía como una serie de tramas de vertimiento único al conjunto reconocido dinámicamente de servidores y direccionadores IPX.

Cuando se habilita la detección de BCM IPX Server Farm, BCM IPX detectará un IPX server farm cuando el número de direccionadores y servidores IPX descubiertos detrás de un LEC determinado excede un umbral configurable, el *Umbral de BCM IPX Server Farm*. Cuando se detecta un server farm, BCM IPX difunde una trama gestionada a cada LEC que representa un server farm, en lugar de transmitir múltiples tramas de vertimiento único a cada direccionador y servidor IPX en sentido directo del server farm. Ahora, BCM IPX puede utilizar inteligentemente el mecanismo de difusión en áreas de la red en las que es deseable hacerlo.

Con BCM IPX habilitado, cualquier dispositivo lacónico (es decir, un dispositivo que no transmite anuncios IPX) que necesite recibir anuncios IPX tiene que configurarse como un destino estático de BCM. Un ejemplo de un dispositivo así es una estación que ejecuta software que descubre la topología de la red IPX supervisando anuncios IPX.

Si se habilita la detección de BCM IPX Server Farm y desea impedir que BCM IPX trate a un LEC en particular como un Server Farm, configure un destino estático BCM con la dirección ATM del LCE y la dirección MAC 00.00.00.00.00.00. Esto fuerza a que BCM IPX envíe tramas gestionadas por BCM como múltiples tramas de vertimiento único a cada direccionador y servidor IPX en sentido directo detectado detrás de este LEC, incluso si el número de direccionadores y servidores detectados excede el *Umbral de BCM IPX Server Farm*.

Soporte BCM para NetBIOS

NetBIOS se considera un protocolo que abusa de las difusiones y, por lo tanto, un excelente candidato para BCM. La comunicación NetBIOS se basa en nombres. Las estaciones que transmiten pueden reconocer la dirección MAC asociada con un nombre de destino en particular difundiendo una consulta o mediante la multidifusión de la trama a la dirección funcional NetBIOS. En el último caso, cada dispositivo NetBIOS de la red debe recibir la trama y determinar si el nombre de destino de la trama se aplica a sí mismo. Para empeorar la situación, los dispositivos NetBIOS tienden a repetir la transmisión de ciertos tipos de tramas hasta 10 veces. Históricamente, lo hacía para asegurarse de que todos los dispositivos recibieran la trama cuando la red estaba muy congestionada.

Visión general de LAN Emulation

La estrategia de BCM es asociar los nombres NetBIOS exclusivos con las direcciones MAC y los clientes LE reconociendo los nombres de las tramas NetBIOS enviadas al BUS. Después de reconocer un nombre NetBIOS exclusivo, las tramas de difusión NetBIOS subsiguientes destinadas a este nombre se reenvían a un solo cliente LE como una trama de vertimiento único. BCM también filtra algunas tramas NetBIOS que se difunden repetidamente.

BCM proporciona soporte para el compartimiento de nombres de NetBIOS. Es decir BCM NetBIOS maneja estaciones OS/2 LANServer con múltiples adaptadores de la LAN que comparten el mismo nombre NetBIOS.

Soporte de BCM para el puente de ruta de origen

La Gestión de ruta de origen (SRM) es una característica adicional de BCM que puede configurarse para las 802.5 ELAN. Cuando está habilitada, esta característica procesará más las tramas gestionadas por BCM IP o BCM NetBIOS y, siempre que sea posible, transformará las tramas Exploradoras de todas las rutas (ARE) o Exploradoras de árbol de expansión (STE) en Tramas específicamente direccionadas (SRF). Cuando una trama se transforma en SRF, la trama ya no necesita transmitirse en cada anillo de la red puenteada.

La topología de Red en Anillo detrás de cada cliente LE se reconoce registrando el campo de información de direccionamiento (RIF) de las tramas recibidas por el BUS. Puesto que SRM reconoce dinámicamente la información de topología de Red en Anillo, se utiliza un mecanismo de antigüedad para eliminar la información que no ha sido renovada recientemente.

Para decidir si habilitar BCM o SRM (o ambos), debe compararse el beneficio en todo el sistema de la red con la reducción inevitable en la velocidad a la que se reenvían los paquetes cuando se habilita BCM o SRM.

Nota: El Gestor de difusión y la Gestión de ruta de origen no están disponibles y no pueden habilitarse si **bus-mode** se establece en *adapter* o en *vcc-splice*.

Fiabilidad de LAN Emulation

Una de las críticas que más se ha proclamado de LAN Emulation ha sido la percepción de una falta de fuerza. Aunque ATM Forum dirige este punto con especificaciones para distribuir el servicio LE, el direccionador ofrece una respuesta. La Figura 18 en la página 307 proporciona una infraestructura para describir la solución de la redundancia MSS.

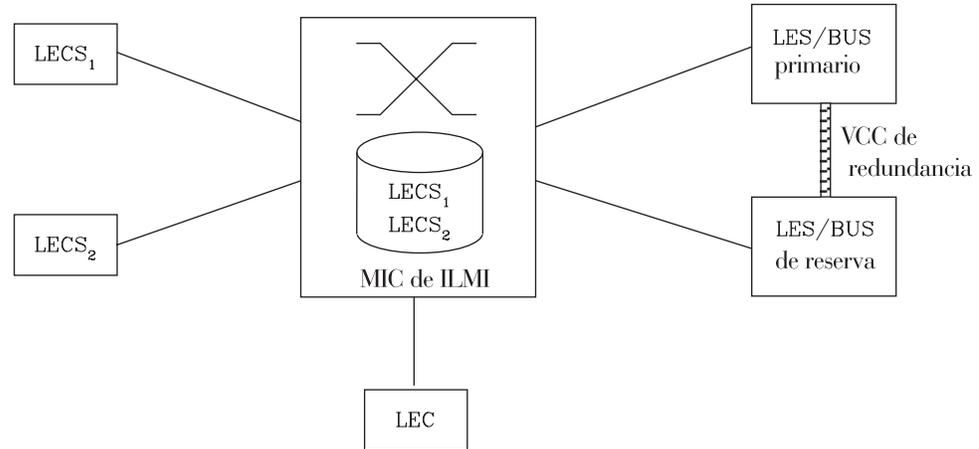


Figura 18. Redundancia de LAN Emulation

Cada LES/BUS puede configurarse independientemente para la redundancia (el valor por omisión es sin redundancia). Si se habilita la redundancia, el LES/BUS se configura para asumir la función de un LES/BUS primario o de reserva. A menos que se haya configurado como LES/BUS redundante, el LES/BUS es primario. Normalmente el LES/BUS primario es el único LES/BUS visible para los clientes LE. Es responsable de configurar y mantener una VCC de redundancia ampliada para el LES de reserva. La presencia de esta VCC y los oportunos mensajes de estado indican que el LES/BUS primario está operativo.

Si la VCC de redundancia ampliada **no** está presente, el LES/BUS de reserva presta servicio a las peticiones de la ELAN de manera normal. Si el LES/BUS de reserva está prestando servicio a la ELAN cuando el primario establece la VCC de redundancia ampliada, el comportamiento se determina por el valor del soporte de redundancia del similar de LES/BUS.

La habilitación del soporte de redundancia del similar permite que los clientes permanezcan activos en el LES/BUS de reserva incluso después de establecer la VCC de redundancia ampliada entre el LES/BUS primario y de reserva. Cuando el soporte de redundancia está habilitado, pero la redundancia del similar está inhabilitada, el LES/BUS de reserva termina todos sus clientes cuando se establece la VCC de redundancia ampliada, siempre conduciendo al LES/BUS primario. Cuando están inhabilitados los soportes de redundancia y de redundancia del similar y la VCC de redundancia ampliada está activada, los LES/BUS primario y de reserva transmiten periódicamente mensajes de estado del uno al otro que contienen el número de clientes activos. En caso de que los LES/BUS primario y de reserva tengan clientes activos en el momento en que se establezca la VCC de redundancia ampliada, el LES/BUS con el menor número de clientes activos termina sus clientes, conduciendo al LES/BUS con el mayor número de clientes activos. Si el número de clientes activos es igual, el LES/BUS de seguridad conduce al primario. Para dar preferencia al LES/BUS primario en la condición de actualización donde el primario y el de reserva pasan a estar operativos aproximadamente a la vez, el de reserva conducirá al primario si la VCC de redundancia ampliada se establece dentro del minuto siguiente a que el de reserva se registre en el conmutador ATM.

Visión general de LAN Emulation

Para simplificar, sólo el LES/BUS primario tiene la opción de redundancia del similar. La redundancia del similar está inhabilitada por omisión para mantener el comportamiento de la redundancia de los releases anteriores del software del direccionador.

Para que el protocolo de redundancia sea eficaz, los clientes LE deben detectar la anomalía del LES/BUS primario y conectarse al de reserva. Los clientes LE detectan las anomalías del servidor por las VCC liberadas. La conexión con el LES/BUS de reserva se realiza a través del LECS.

Cuando se recibe una petición LE_CONFIGURE_REQUEST, el LECS asigna el cliente LE al LES y ELAN adecuados. Si este LES no tiene configurada ningún LES de reserva, el LECS devuelve la dirección ATM del LES. Si el LES tiene configurado un LES de reserva, el LECS devuelve la dirección del LES primario o de reserva.

El LECS devuelve la dirección del LES de reserva si existe el LES de reserva en el mismo MSS Server que el LECS y está sirviendo actualmente a la ELAN, si existe el LES primario en el mismo MSS Server que el LECS y no está sirviendo actualmente a la ELAN, o si no existe el LES en el mismo MSS Server que el LECS y el cliente se asignó la última vez al LES primario (dentro de los 5 últimos minutos). De lo contrario, devuelve la dirección del LES primario al cliente LE.

El LECS conserva una memoria a corto plazo de todas las asignaciones de clientes de modo que puede dirigir alternativamente un cliente LE a un LES primario y de reserva. Esta heurística simple realiza la asignación correcta en el caso nominal de que no se haya producido ninguna anomalía y se corrige a sí misma. En el peor de los casos, la heurística hace que el cliente LE repita la fase de configuración de la unión a una ELAN.

La fuerza de LECS puede conseguirse estableciendo LECS duplicados en múltiples plataformas e incluyendo sus direcciones ATM en la base de datos ILMI. Los clientes LE se conectarán entonces al LECS de reserva si el primario no está disponible. podrían estar en MSS Server 1, mientras

Seguridad de LAN Emulation

Las LAN tradicionales ofrecen seguridad en el sentido de que una conexión física implica que dos estaciones están en la misma LAN. Puesto que pueden existir múltiples LAN emuladas en una sola red ATM, las estaciones que no están en la ELAN pueden conectarse físicamente a estaciones que están en la ELAN. Esta situación presenta el riesgo de seguridad de que puedan conectarse estaciones no autorizadas al LES e intentar utilizar sus servicios.

Para controlar los miembros de la ELAN, puede configurarse un MSS LES para validar las peticiones LE_JOIN_REQUEST en los LECS. En esta modalidad, el LES forma una petición LE_CONFIGURE_REQUEST en nombre del cliente LE utilizando la información de la petición LE_JOIN_REQUEST. Estas peticiones LE_CONFIGURE_REQUEST incluyen el destino de LAN de origen, la dirección ATM de origen, el tipo de ELAN, el tamaño máximo de trama y el nombre de ELAN de la petición. LE_JOIN_REQUEST, junto con un TLV de seguridad IBM. Las peticiones de seguridad se transmiten al LECS mediante un componente de multiplexión llamado interfaz LECS y el LECS debe validar las peticiones utilizando su base de datos de asignaciones de ELAN antes de que los clientes LE tengan permitido unirse a la ELAN.

Visión general de LAN Emulation

Se asocia una interfaz LECS con una interfaz ATM y todos los LES configurados en la interfaz ATM utilizan la misma interfaz LECS. La interfaz LECS conserva los recursos de VCC mediante la multiplexión de las peticiones de seguridad de múltiples LES en una sola VCC para el LECS. La interfaz LECS localiza los LECS dinámicamente utilizando la ILMI y los mecanismos conocidos de dirección LECS. Después de establecer la VCC con el LECS, la interfaz LECS emite una consulta local para determinar si el LECS está ubicado en el mismo direccionador. Si el LECS está ubicado en el mismo direccionador, se utiliza una interfaz local para confirmar las peticiones de unión sin transmitir peticiones a la red ATM.

Con la interfaz LECS, el direccionador puede asegurar que un cliente LE se une a una ELAN sólo si el LECS aprueba la unión. Esto desplaza la carga de la seguridad del LES al LECS. Desafortunadamente, el LECS tampoco es seguro. El LECS acepta las conexiones y consultas de cualquier estación sin verificación. Una estación intrusa puede conectarse al LECS y consultar repetidamente varias configuraciones. El intruso también puede actuar como cualquier otra estación y descargar la configuración de otra estación.

Los controles de acceso al LECS permiten que el usuario configure una lista de prefijos de direcciones ATM que no tienen permitido acceder a la base de datos de configuración del LECS. Todos los intentos de conexión al LECS y las peticiones LE_CONFIGURE_REQUEST de las direcciones ATM coincidentes se rechazan automáticamente. Cuando se utilizan con la interfaz LECS, se proporciona un entorno de LAN seguro.

Para maximizar la seguridad de una ELAN, se recomiendan los pasos siguientes:

1. En el LECS, utilice direcciones ATM para asignar clientes al LES. Consulte la sección "Visión general de la función LECS" en la página 296 para obtener más información.
2. Active la Interfaz LECS en el direccionador.
3. Active la opción de seguridad de los LES.
4. Active los Controles de acceso al LECS para cualquier prefijo de dirección ATM que no deba tener permitido acceder al LECS.
5. Utilice *Address Screening* en los conmutadores ATM. Esta opción hace que los conmutadores validen que las estaciones que llaman utilicen sus direcciones ATM reales en la configuración de la llamada. Por lo tanto, las estaciones no pueden suplantar a otras estaciones.

Estos pasos aseguran que las estaciones estén correctamente identificadas y que sólo las estaciones autorizadas se unan a la ELAN.

Interfaz de red a red de LAN Emulation (LNNI)

Parámetros clave de configuración para LAN Emulation

Esta sección describe brevemente los parámetros de configuración necesarios de los componentes de LAN Emulation del direccionador. Debe definirse la interfaz ATM para los componentes de LAN Emulation antes de que puedan crearse los componentes.

1. LEC:

Para crear un cliente LE, sólo tiene que especificar el tipo de ELAN. Si define dos clientes LE en una sola interfaz ATM y tiende un puente para los dos juntos, uno de los clientes LE debe utilizar una dirección del MAC diferente del

Visión general de LAN Emulation

valor por omisión. Por omisión, los clientes LE utilizan la dirección del MAC incorporada de la interfaz ATM. El tamaño de trama máximo por omisión es de 1516 bytes para los clientes LE Ethernet y de 4544 bytes para los clientes LE Red en Anillo.

Capítulo 24. Utilización de ATM

Este capítulo describe cómo utilizar la interfaz ATM. Incluye las secciones siguientes:

- “ATM y LAN Emulation”
- “Cómo entrar direcciones”
- “Multiplexación ATM-LLC” en la página 312
- “Conceptos de interfaz virtual ATM” en la página 312

ATM y LAN Emulation

LAN Emulation proporciona soporte para las LAN de Red en Anillo y Ethernet virtuales a través de una red ATM. Consulte la sección “Cómo entrar direcciones” para ver una explicación del direccionamiento ATM.

Cómo entrar direcciones

Entre las direcciones de dos maneras, dependiendo de si la dirección representa (1) una dirección IP o (2) una dirección ATM, una dirección MAC, o un descriptor de ruta, o una dirección MAC, de la manera siguiente:

1. Dirección IP

Entre las direcciones IP en formato decimal con puntos, un campo de 4 bytes representados por cuatro números decimales (de 0 a 255) separados por puntos (.).

Ejemplo de dirección IP:

01.255.01.00

2. Dirección ATM o MAC o descriptor de ruta

Entre las direcciones ATM, las direcciones MAC y los descriptors de rutas como series de caracteres hexadecimales con o sin caracteres separadores opcionales entre bytes. Los caracteres separadores válidos son guiones (-), puntos (.) o dos puntos (:).

Ejemplos de dirección ATM, dirección MAC o descriptor de ruta

A1FF01020304

o

A1-FF-01-02-03-04

o

A1.FF.01.02.03.04

o

39.84.0F.00.00.00.00.00.00.00.00.00.00.03.10.00.5A.00.DE.AD.08

o

A1:FF:01:02:03:04

o incluso

A1-FF.01:0203:04

Cada tipo de dirección necesita un número diferente de caracteres hexadecimales:

ATM 40

MAC 12

ESI 12

Descriptor de ruta

4

Esta información se aplica a las direcciones entradas para ATM, LAN emulation, Classical IP y ARP a través de ATM, IPX a través de ATM y ARP a través de ATM.

Multiplexación ATM-LLC

Los protocolos que se ejecutan nativamente a través de una interfaz ATM pueden utilizar la multiplexación ATM-LLC para compartir las direcciones ATM y los canales SVC y PVC entre los usuarios. ATM-LLC se configura implícitamente cuando se configuran los protocolos y puede supervisarse utilizando el indicador de mandatos ATM Config+ de **t 5**. No hay ninguna opción de configuración explícita para la función de multiplexación ATM-LLC. Por ejemplo, si dos protocolos que utilizan la multiplexación ATM-LLC están configurados para utilizar la misma dirección ATM local (punto final local), esto configura implícitamente ATM-LLC para que utilice la misma dirección ATM compartida para ambos protocolos.

Consulte la sección “Mandatos de supervisión ATM-LLC” en la página 327 para obtener información adicional.

El compartimiento de las direcciones ATM o de canales SVC/PVC no es posible entre protocolos que utilizan la función de multiplexación ATM-LLC y los que no utilizan la función de multiplexación ATM-LLC (por ejemplo, Classical IP). Actualmente, Server Cache Synchronization Protocol (SCSP) y APPN son los dos únicos protocolos que utilizan la función de multiplexación ATM-LLC.

Conceptos de interfaz virtual ATM

Una Interfaz virtual ATM (AVI) crea la apariencia de múltiples interfaces ATM cuando, de hecho, sólo hay una interfaz física ATM. Se pueden configurar una o varias AVI para cada interfaz física ATM en el dispositivo. Las AVI tienen las características siguientes:

- Cada AVI debe estar definida en una (y sólo una) interfaz física ATM. La interfaz real ATM (ARI) se utilizará para significar la interfaz física ATM.
- Se pueden configurar una o varias AVI en cada ARI de un dispositivo.
- Los protocolos de capas superiores tratan las ARI y las AVI de igual forma. Los protocolos ven el número total de interfaces ATM como la suma de las ARI y AVI configuradas en el dispositivo.
- Los protocolos pueden configurarse en cada interfaz ATM (real o virtual) independientemente de otras interfaces.

Por ejemplo, el usuario puede configurar IP en la interfaz 0 (que es una interfaz ATM real) con la dirección IP 9.1.1.1 y otra instancia de IP con la dirección 9.2.1.1 en la interfaz 1 (que es una AVI). Si una interfaz es una interfaz ATM real o una interfaz virtual configurada en una interfaz real no tiene ninguna importancia para el protocolo (IP en el ejemplo). Además, si la interfaz virtual 1 está configurada en la parte superior de la interfaz ATM 0 real o alguna otra interfaz física ATM también es transparente para los protocolos.

Ventajas de utilizar las interfaces virtuales ATM

Las principales ventajas de utilizar las interfaces virtuales ATM son:

- La utilización de la característica de Interfaz virtual ATM aumenta el número de instancias de protocolo que se pueden soportar en una interfaz física ATM.

El número real de AVI que se puede configurar en una ARI está limitado por los recursos físicos, como la memoria, disponibles en el dispositivo. El número total de interfaces que se pueden crear depende del tamaño del paquete de datos para las interfaces y está limitado a un número máximo de 253 por dispositivo.

La utilización de las AVI mejora significativamente las opciones de configuración para los protocolos como IPX que están limitados a una instancia o dirección por

Conceptos de configuración de interfaz virtual ATM

interfaz ATM. Mediante la configuración del número adecuado de AVI, se pueden soportar varias direcciones IPX en cada interfaz física ATM.

- La característica de Interfaz virtual ATM es importante para soportar los protocolos de direccionamiento de multidifusión (como MOSPF) a través de las redes ATM.

Para que la multidifusión funcione correctamente, cada subred lógica **debe** estar configurada en una interfaz diferente porque los protocolos de direccionamiento de multidifusión normalmente funcionan de tal manera que un paquete que viene de una interfaz de dispositivo no se enviará a través de la misma interfaz. Por lo tanto, si se configura más de una subred en una interfaz y un origen de una subred envía un paquete de multidifusión a un miembro de otra subred definido en la misma interfaz, este miembro no recibirá nunca el paquete.

Creando una interfaz virtual individual para cada subred, se puede realizar la multidifusión de paquetes satisfactoriamente. Normalmente, el número de interfaces ATM de un dispositivo estará limitado, limitando a su vez el número de subredes que pueden configurarse correctamente para el funcionamiento de la multidifusión. Sin embargo, si se crean tantas AVI como sea necesario (de acuerdo al número de subredes que necesitan configurarse en el dispositivo), el número de interfaces físicas ATM ya no limitará el número de subredes que pueden configurarse en un dispositivo para un funcionamiento correcto de la multidifusión.

Por ejemplo, el direccionador de “un brazo” no puede soportar el tráfico de multidifusión a través de interfaces que no sean ELAN sin la característica AVI, porque los paquetes de entrada no se enviarán nunca a la misma interfaz y se eliminarán en su lugar.

- La creación de múltiples AVI en una ARI y la configuración de cada instancia de protocolo diferente (por ejemplo, cada subred IP) en una AVI diferente de la misma ARI, puede mejorar el rendimiento.

Por ejemplo, cuando se configuran múltiples subredes en una sola interfaz física ATM, la interfaz tendrá que reducir la unidad de transmisión máxima o MTU (el tamaño máximo de paquete que puede enviarse o recibirse a través de esta interfaz) a la MTU más pequeña de todas las subredes que comparten la misma interfaz. Sin embargo, si se crean múltiples AVI en esa ARI y cada subred IP se configura en una AVI diferente, cada subred puede continuar utilizando su tamaño de MTU existente sin tomar en consideración las demás subredes configuradas en la misma interfaz física ATM. Esto evita la posible reducción de la productividad y los retardos debido a la fragmentación y reensamblaje de paquetes provocado por la reducción del tamaño de MTU.

Puede conseguirse otra mejora del rendimiento distribuyendo el número de direcciones de protocolo configuradas en una interfaz física a través de diferentes interfaces virtuales configuradas en la misma interfaz física. Las listas de protocolos por interfaz se reducen, dando como resultado búsquedas más rápidas y un tiempo de proceso reducido.

Desventajas de utilizar las interfaces virtuales ATM

Las desventajas de utilizar las interfaces virtuales ATM son:

- Puesto que las AVI no tienen sus propios recursos físicos, cada interfaz virtual puede tener menos Conexiones virtuales (VC) que una sola interfaz física. Los recursos disponibles (en este ejemplo las VC) se particionan entre las distintas interfaces virtuales configuradas de una sola ARI y la ARI en sí.

En la implementación actual, la asignación de recursos es *a petición*. Cada interfaz física ATM tiene una agrupación de recursos que están disponibles para que todas las AVI y la única ARI los utilicen.

Conceptos de configuración de interfaz virtual ATM

Nota: Puesto que todos los recursos se comparten entre la ARI y todas las AVI, un ESI añadido a una ARI está disponible automáticamente para todas las AVI configuradas en la ARI. No debe asignar la misma combinación de ESI y selector a dos clientes diferentes del protocolo que utilicen la misma ARI aunque estén configurados en AVI diferentes.

Se permite el compartimiento limitado de PVC en la ARI y en las AVI configuradas en la ARI. El compartimiento de PVC está limitado para las instancias diferentes del protocolo. No se permite que múltiples instancias del mismo protocolo compartan el mismo PVC.

Capítulo 25. Configuración y supervisión de ATM

Este capítulo describe los mandatos de configuración y operativos de la interfaz ATM. Incluye las secciones siguientes:

- “Acceso al proceso de configuración de la interfaz ATM”
- “Mandatos de configuración ATM”
- “Mandatos de configuración de interfaces ATM” en la página 316
- “Mandatos de configuración de interfaz virtual ATM” en la página 322
- “Mandatos de supervisión de interfaz virtual ATM” en la página 328
- “Acceso al proceso de supervisión de ATM” en la página 323
- “Mandatos de supervisión ATM” en la página 324
- “Mandatos de supervisión de la interfaz ATM (indicador ATM INTERFACE+)” en la página 325
- “Mandatos de supervisión ATM-LLC” en la página 327
- “Soporte para la reconfiguración dinámica de ATM y ATM virtual” en la página 328

Acceso al proceso de configuración de la interfaz ATM

Utilice el procedimiento siguiente para acceder al proceso de configuración.

1. En el indicador OPCON, entre **talk 6**. (Para ver los detalles de este mandato, consulte la sección “¿Qué es el proceso OPCON?” en la página 33.) Por ejemplo:

```
* talk 6
  Config>
```

Se visualiza el indicador CONFIG (Config>) en la consola. Si no aparece el indicador cuando entre en la configuración, pulse **Intro** de nuevo.

2. En el indicador CONFIG, entre el mandato **list devices** para visualizar los números de las interfaces de red para las que el dispositivo está configurado actualmente.
3. Anote los números de interfaz. Si no se especifica ATM como interfaz, cree una interfaz ATM utilizando el mandato **add device** en el indicador Config>.
4. Entre el mandato **network** y el número de interfaz ATM que desea configurar. Por ejemplo:

Se visualiza el indicador de configuración ATM (ATM Config>).

Mandatos de configuración ATM

Esta sección resume los mandatos de configuración ATM. Entre los mandatos en el indicador ATM config>.

Tabla 39. Resumen de los mandatos de configuración ATM

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página 10.

Mandatos de configuración ATM (Talk 6)

Tabla 39. Resumen de los mandatos de configuración ATM (continuación)

Mandato	Función
Interface	Visualiza el indicador ATM Interface Config> desde el cual puede listar, cambiar o configurar la Interfaz ATM. <ul style="list-style-type: none"> • Añade un ESI. • Lista la configuración actual o lista los ESI. • Elimina un ESI. • Establece los parámetros de la red ATM. • Habilita o inhabilita un ESI. • Sale
Le-client	Visualiza el indicador LE Client Config> desde el cual puede listar, cambiar o configurar la interfaz LAN Emulation Client, descrita en la sección “Capítulo 26. Utilización de los LAN Emulation Client” en la página 331. <ul style="list-style-type: none"> • Añade un LAN Emulation Client (LEC) para una LAN emulada de red en anillo o de Ethernet. • Configura un LEC por número de red. Este mandato visualiza el indicador LE Config> desde el que puede configurar un LAN Emulation Client (LEC) específico. • Lista los LAN Emulation Client (LEC). • Eliminar un LAN Emulation Client (LEC).
Virtual ATM	Visualiza el indicador ATM Virtual Interface Config> desde el cual puede listar, añadir o eliminar la Interfaz virtual ATM, tal como se describe en la sección “Mandatos de configuración de interfaz virtual ATM” en la página 322
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página 11.

Mandatos de configuración de interfaces ATM

Esta sección resume y explica los mandatos para configurar una interfaz ATM específica.

Entre los mandatos en el indicador ATM INTERFACE>.

Tabla 40. Resumen de los mandatos de configuración de interfaces ATM

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página 10.
Add	Añade un ESI.
List	Lista la configuración actual o los ESI.
Qos	Visualiza el indicador ATM I/F 0 QOS Config> desde el cual puede configurar la Calidad de los servicios, tal como se describe en la sección “QoS Configuration” en la página 317.
Remove	Elimina un ESI.
Set	Establece los parámetros de la red ATM.
Disable	Inhabilita un ESI.
Enable	Habilita un ESI.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página 11.

Add

Utilice el mandato **add** para añadir un ESI a la configuración ATM.

Los octetos 14–19 de una dirección ATM son el Identificador del sistema final (ESI). Cada sistema final conectado al mismo conmutador debe utilizar un conjunto inconexo de ESI. Cuando se activa un sistema final, intenta registrar sus ESI en su conmutador ATM utilizando ILMI. El conmutador obliga a que todos sus ESI registrados sean exclusivos.

Sintaxis:

add esi *dirección-esi*

esi *dirección-esi*

La dirección del Identificador del sistema final.

Valores válidos:

Cualquier combinación de 12 dígitos hexadecimales

Valor por omisión:

ninguno

List

Utilice el mandato **list** para listar la configuración de este dispositivo ATM o para listar el conjunto de ESI configurados.

Sintaxis:

list configuration

esi

configuration

Lista la configuración del dispositivo ATM. Para ver una explicación de los campos listados, consulte la sección “Set” en la página 318.

Ejemplo: list con

ATM Configuration

```
Interface (net) number = 0
Maximum VCC data rate Mbps = 155
Maximum frame size = 9234
Maximum number of callers = 209
Maximum number of calls = 1024
Maximum number of parties to a multipoint call = 512
Maximum number of Selectors that can be configured = 200
UNI Version = UNI 3.0
Packet trace = OFF
```

esi Lista los ESI de la configuración ATM.

Ejemplo: list esi

ATM INTERFACE> **list esi**

ESI	Enabled
000000000009	YES
000000000100	YES

QoS Configuration

Utilice el mandato **qos-configuration** para visualizar el indicador ATM I/F 0 QOS Config> desde el cual puede configurar la calidad de los servicios, tal como se describe en la sección “QoS Configuration”.

Mandatos de configuración de interfaces ATM (Talk 6)

Sintaxis:

qos-configuration

Remove

Utilice el mandato **remove** para eliminar un ESI de la configuración ATM. Todos los componentes ATM que utilizan este ESI se deben volver a configurar para que utilicen otro ESI distinto. Es posible que, en el siguiente reinicio del dispositivo, no se active un componente ATM que intente utilizar un ESI eliminado.

Sintaxis:

remove esi dirección-esi

esi dirección-esi

La dirección del Identificador del sistema final.

Valores válidos:

Cualquier combinación de 12 dígitos hexadecimales

Valor por omisión:

ninguno

Set

Utilice el mandato **set** para especificar los parámetros de red ATM.

Sintaxis:

set max-callers
max-calls
max-config-selectors
max-data-rate
max-frame
max-mp-parties
network-id
trace
uni-version

max-callers

Establece el número máximo de entidades del dispositivo que utilizan la interfaz ATM. Cada interfaz LEC, Classical IP Client y puente 1483 se califica como usuario de la interfaz ATM. Aumentando este parámetro permite que haya más usuarios de la interfaz y utiliza más memoria del sistema.

Valores válidos:

Un entero en el rango de 64 a 1024

Valor por omisión:

209

Ejemplo:

```
ATM INTERFACE> set max-callers 25
```

max-calls

Establece el número máximo de circuitos virtuales conmutados (SVC) que pueden existir en este dispositivo ATM. Cada SVC de punto a punto y de

Mandatos de configuración de interfaces ATM (Talk 6)

punto a multipunto utiliza recursos del sistema. Este parámetro ayuda a limitar los recursos del sistema reservados para las conexiones de señalización y conmutadas. Al aumentar este parámetro permitirá más SVC simultáneos. Sin embargo, se necesitará más memoria del sistema para gestionar estas conexiones.

Valores válidos:

Un entero en el rango de 64 a 10500

Valor por omisión:

1024

Ejemplo:

```
ATM INTERFACE> set max-calls 500
```

max-config-selectors

Establece el número máximo de selectores bajo su control específico.

El selector se utiliza para distinguir los diferentes usuarios del mismo sistema final. Las peticiones de configuración de VCC se dirigen de la siguiente manera jerárquica: los conmutadores ATM dirigen al conmutador ATM de destino utilizando el Prefijo de red, el conmutador ATM de destino dirige al sistema final de destino utilizando el ESI y el sistema final notifica al usuario de destino basándose en el selector.

Cada ESI puede tener hasta 255 selectores asociados (de 0x00 a 0xff). El rango de selectores se divide en dos subrangos, un rango de selectores configurados y un rango de selectores asignados automáticamente. El parámetro de la interfaz ATM max-configured-selector proporciona el límite superior del rango de selectores configurados.

Los componentes ATM del dispositivo tienen varias maneras de elegir un selector. Algunos componentes necesitan que el usuario configure explícitamente un selector del rango de selectores configurados. Otros componentes, por ejemplo, clientes Classical IP, permiten que el selector se asigne automáticamente en tiempo de ejecución. No tiene que elegir el selector porque el dispositivo lo hace cuando se activa. No se garantiza la coherencia de este selector en los reinicios del dispositivo. La asignación automática del selector sólo es útil para los componentes ATM cuya dirección ATM no tiene que ser conocida aún por otros dispositivos de la red.

Los tamaños relativos del rango de selectores pueden modificarse para que se ajusten a los tipos y números de usuarios ATM del dispositivo.

Valores válidos:

De 0 a 255 (0x00 – 0xFF)

Valor por omisión:

200

Nota: El selector es el byte 20 de una dirección ATM de 20 bytes.

Ejemplo:

```
ATM INTERFACE> set max-config-selectors 225
```

max-data-rate *velocidad*

Establece el límite por omisión y superior para los parámetros de tráfico de VCC de la mayoría de conexiones LANE y CIP. Por ejemplo, este es el PCR por omisión para las VCC de mejor esfuerzo iniciadas por LE Clients. Los SCR y PCR señalados no puede exceder este límite. El valor por omisión debe ser satisfactorio en la mayoría de situaciones. Un ejemplo de una situación en la que es beneficioso cambiar este valor sería si la

Mandatos de configuración de interfaces ATM (Talk 6)

mayoría de estaciones utilizan adaptadores de 25 Mbps. En este caso, podría ser aconsejable limitar la velocidad de los datos de las VCC a 25 Mbps para que las estaciones de velocidad inferior no se abrumen con tramas del dispositivo. Las unidades para este parámetro son Mbps.

Valores válidos:

25
100
155

Valor por omisión:

155

Ejemplo:

```
ATM INTERFACE> set speed 155
```

max-frame

Establece el número máximo de octetos permitidos en cualquier trama de datos enviada o recibida en la interfaz ATM. La memoria del sistema se asigna basándose en este parámetro. El aumento de max-frame necesita más memoria del sistema, pero permite el proceso de tramas mayores.

Todas las entidades de dispositivo que utilicen la interfaz ATM deben utilizar un tamaño de trama máximo menor o igual a max-frame-size de la interfaz ATM. Esto incluye todas las interfaces LEC y de puente 1483.

Valores válidos:

Un entero en el rango de 512 a 31000

Valor por omisión:

9234

Ejemplo:

```
ATM INTERFACE> set max-frame 1000
```

max-mp-parties

Establece el número máximo de hojas en una conexión de punto a multipunto iniciada por el dispositivo. Este parámetro afecta a la asignación de memoria del sistema. Es necesario aumentar este valor si el dispositivo debe configurar conexiones de punto a multipunto para una gran número de destinos.

Valores válidos:

Un entero en el rango de 1 a 5000

Valor por omisión:

512

Ejemplo:

```
ATM INTERFACE> set max-mp-parties 300
```

network-id

Establece el id de red de la interfaz ATM. Múltiples interfaces ATM deben tener el mismo id de red si hay una conectividad ATM entre las interfaces.

Valores válidos:

De 0 a 255

Valor por omisión:

0

trace Establece los parámetros de rastreo de paquetes en la interfaz. El rastreo de paquetes se puede habilitar o inhabilitar en un rango de valores VPI/VCI. Los valores VPI/VCI comunes para el rastreo son:

- De 0 a 5 para paquetes de señalización.
- De 0 a 16 para paquetes ILMI.

Mandatos de configuración de interfaces ATM (Talk 6)

Valores válidos:

on, off

Valor por omisión:

off

Se le solicita el rango VPI/VCI que desea rastrear.

Valores válidos de VPI de inicio:

De 0 a 255

Valor por omisión:

0

Valores válidos de VPI de fin:

De 0 a 255

Valor por omisión:

255

Valores válidos de VCI de inicio:

De 0 a 65535

Valor por omisión:

0

Valores válidos de VCI de fin:

De 0 a 65535

Valor por omisión:

65535

Ejemplo:

```
ATM INTERFACE> set trace on
beginning of VPI range [0]? 0
end of VPI range [255]? 0
beginning of VCI range [0]? 5
end of VCI range [65535]? 5
```

uni-version

Establece la versión de User Network Interface (UNI) utilizada por la interfaz ATM cuando se comunica con el conmutador ATM conectado. Si las versiones de UNI están configuradas en el conmutador ATM y en la interfaz de dispositivo ATM para una versión específica (que no sea AUTO-DETECT), las versiones de UNI deben coincidir.

Si la versión de UNI está configurada como AUTO, el dispositivo ATM intenta conocer la versión UNI que se ha de utilizar del conmutador.

En modalidad UNI AUTO-DETECT, si el conmutador no responde a la consulta de la versión de UNI, el valor por omisión es UNI 3.0. Si el conmutador responde con otro valor distinto de UNI 3.0 o UNI 3.1, el valor por omisión es UNI 3.1.

Valores válidos:

[UNI 3.0|UNI 3.1|AUTO-DETECT|Ninguno]

Valor por omisión:

UNI 3.0

Nota: Debe ser compatible con el conmutador ATM.

Ejemplo:

```
ATM INTERFACE> set uni-version 3.0
```

Enable

Utilice el mandato **enable** para habilitar un ESI de la configuración del dispositivo ATM. La interfaz ATM intenta registrar únicamente los ESI habilitados cuando se activa.

Mandatos de configuración de interfaces ATM (Talk 6)

Sintaxis:

enable esi dirección-esi

esi dirección-esi

La dirección de los Identificadores del sistema final.

Valores válidos:

Cualquier combinación de 12 dígitos hexadecimales

Valor por omisión:

ninguno

Ejemplo: enable esi

```
ATM INTERFACE> enable esi 00:00:00:00:00:09
```

Disable

Utilice el mandato **disable** para inhabilitar un ESI en la configuración. Los componentes ATM que utilizan ESI inhabilitados no se activarán en el siguiente reinicio del dispositivo.

Sintaxis: disable esi dirección-esi

esi dirección-esi

La dirección de los Identificadores del sistema final.

Valores válidos:

Cualquier combinación de 12 dígitos hexadecimales

Valor por omisión:

ninguno

Ejemplo: disable esi

```
ATM INTERFACE> disable esi 00:00:00:00:00:09
```

Acceso al proceso de configuración de interfaz virtual ATM

En el indicador ATM Config> de una interfaz real ATM seleccionada, utilice el mandato **Virtual ATM** para entrar en la modalidad de mandatos de configuración de ATM virtual.

Mandatos de configuración de interfaz virtual ATM

Esta sección resume los mandatos de configuración de interfaz virtual ATM. Entre los mandatos en el indicador ATM virtual interface config>.

Tabla 41. Resumen de los mandatos de configuración de interfaz virtual ATM

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado "Cómo obtener ayuda" en la página 10.
Add	Añade una interfaz virtual ATM.
List	Lista las interfaces virtuales ATM configuradas actualmente.
Remove	Elimina la interfaz virtual ATM de la configuración actual.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página 11.

Add

Utilice el mandato **add** para añadir una interfaz virtual ATM. Se añade una nueva interfaz virtual ATM a la interfaz real ATM correspondiente (el menú de configuración desde el cual se accede a este menú de configuración de interfaces virtuales ATM). Se visualiza el número de red/interfaz asignado a la interfaz virtual ATM que se acaba de crear y es un número mayor que el número mayor de interfaz actual.

Sintaxis:

add

Ejemplo:

```
ATM Virtual Interface config> add
Added ATM Virtual Interface Net as interface 5 on physical ATM interface 0
ATM Virtual Interface config>
```

List

Utilice el mandato **list** para listar las interfaces virtuales ATM configuradas definidas en la interfaz real ATM actual.

Sintaxis:

list

Ejemplo:

```
ATM Virtual Interface config> list

-----
                        ATM Virtual Interface Nets
-----
ATM interface number = 0
ATM Virtual Interface Net interface number = 5
ATM Virtual Interface config>
```

Remove

Utilice el mandato **remove** para suprimir una interfaz virtual ATM. Se eliminará la interfaz virtual ATM de la interfaz real ATM con el número de interfaz especificado de los registros de configuración SRAM. Si no especifica un número de interfaz, se suprimirá la última interfaz virtual ATM de esta interfaz real ATM. Si entra un signo de interrogación (?), se listan todas las interfaces virtuales ATM de la interfaz real ATM actual y puede seleccionar en esa lista la interfaz que desea eliminar.

Sintaxis:

remove *n*

Ejemplo: remove 5

```
Virtual ATM 5 deleted successfully.
ATM Virtual Interface config>
```

Acceso al proceso de supervisión de ATM

Utilice el procedimiento siguiente para acceder a los mandatos de supervisión ATM. Este proceso le otorga acceso al proceso de *supervisión* de una ATM.

1. En el indicador OPCON, entre **talk 5**. (Para ver los detalles de este mandato consulte la sección “¿Qué es el proceso OPCON?” en la página 33.) Por ejemplo:

Mandatos de configuración de interfaz virtual ATM (Talk 6)

```
* talk 5  
+
```

Se visualiza el indicador GWCON (+) en la consola. Si no aparece el indicador cuando entre en la consola, pulse **Intro** de nuevo.

2. Entre **interface** en el indicador + para visualizar una lista de las interfaces configuradas.
3. Anote los números de interfaz.
4. Entre **network** seguido del número de la interfaz ATM.

```
+ network 1  
ATM+
```

Se visualiza el indicador de supervisión ATM (ATM+).

Mandatos de supervisión ATM

Esta sección resume los mandatos de supervisión ATM para supervisar las interfaces ATM. Entre los mandatos en el indicador ATM+.

Tabla 42. Resumen de los mandatos de supervisión ATM

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página 10.
Interface	Visualiza el indicador ATM Interface+ desde el cual puede supervisar la interfaz ATM, tal como se describe en la sección “Mandatos de supervisión de la interfaz ATM (indicador ATM INTERFACE+)” en la página 325.
Atm-llc	Visualiza el indicador ATM LLC+ desde el cual puede supervisar los puntos finales, un conjunto de clientes de usuario y un conjunto de canales ATM.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página 11.

Interface

Visualiza el indicador ATM Interface+, descrito en la sección “Mandatos de supervisión de la interfaz ATM (indicador ATM INTERFACE+)” en la página 325.

Sintaxis:

interface

ATM-LLC

Visualiza el indicador ATM-LLC+, descrito en la sección “Mandatos de supervisión ATM-LLC” en la página 327.

Sintaxis:

atm-llc

Mandatos de supervisión de la interfaz ATM (indicador ATM INTERFACE+)

Esta sección resume y explica los mandatos para la supervisión de una interfaz ATM específica.

Entre los mandatos en el indicador ATM INTERFACE+.

Tabla 43. Resumen de los mandatos de supervisión de interfaces ATM

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página 10.
List	Lista las direcciones ATM y las VCC.
Trace	Inicia/Detiene el rastreo de paquetes en el rango especificado de VPI/VCI. El rastreo se puede visualizar por ELS.
Wrap	Inicia/Detiene una prueba de bucle de retorno en la VCC.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página 11.

List

Utilice el mandato **list** para listar diversas categorías de datos ATM.

Sintaxis:

list addresses
all
circuit
vccs
reserved-bandwidth

addresses

Lista las direcciones ATM, junto con un nombre descriptivo, que se utilizan en el dispositivo.

Ejemplo:

ATM INTERFACE+ **list addresses**

```

----- ATM Address ----- Name -----
399999999999999900009999020000041347391804 LEC 1 'eth1'
399999999999999900009999020000041347391802 LES/BUS 'eth1'
```

all

Lista todos los elementos siguientes:

- Direcciones
- Estadísticas de circuitos
- VCC
- Ancho de banda reservado

circuit

Lista las estadísticas para una VCC determinada especificando el par VCI-VPI en particular. También puede especificar el circuito en la línea de mandatos; por ejemplo: list circuit 33.

Ejemplo:

```

ATM INTERFACE+ list circuit
VPI [0]?
VCI [32]?33
```

Mandatos de supervisión de la interfaz ATM (Talk 5)

```
Frames transmitted = 2 Bytes transmitted = 216
Frames received   = 2 Bytes received   = 216
```

vccs Lista todas las VCC establecidas por el dispositivo. Las VCC pueden ser permanentes (PVC) o conmutadas (SVC), de punto a punto o de punto a multipunto y cada una se identifica por un VPI/VCI exclusivo. El mandato trace utiliza el valor de VPI/VCI de una VCC para realizar el rastreo de paquetes en una VCC en particular.

Ejemplo:

P-P VCC de punto a punto

P-MP VCC de punto a multipunto

ILMI VCC de Interim Local Management Interface

SAAL VCC de señalización

Bx-y VCC vinculada internamente a VPI x, VCI y

Sx-y VCC unida internamente a VPI x, VCI y

reserved-bandwidth

Lista el ancho de banda reservado en la interfaz ATM.

Ejemplo:

```
ATM INTERFACE+ list reserved-bandwidth
Line Rate           : 155000 Kbps
Peak Reserved Bandwidth : None
Sustained Reserved Bandwidth : None
```

Trace

Utilice el mandato **trace** para activar el rastreo de paquetes en un rango especificado de valores de VPI/VCI. Puede ver los datos de rastreo utilizando ELS, tal como se describe en la sección “View” en la página 201.

Sintaxis:

```
trace                list
                       on
                       off
```

list Visualiza las opciones actuales del rastreo de paquetes de la interfaz ATM.

Ejemplo:

```
ATM Interface+ trace
on | off | list []? list
Packet trace is ON
Range of VPIs to be traced:    0 -    0
Range of VCIs to be traced:   32 -   39
```

on Inicia el rastreo de paquetes en todas las VCC activas dentro del rango de VPI/VCI especificado.

Ejemplo:

```
ATM Interface+ trace on
beginning of VPI range [0]?
end of VPI range [0]?
beginning of VCI range [32]?
end of VCI range [65535]? 39
```

off Detiene el rastreo de paquetes en todas las VCC.

Ejemplo:

Mandatos de supervisión de la interfaz ATM (Talk 5)

```
ATM Interface+ trace off
ATM Interface+ trace list
Packet trace is OFF
```

Wrap

Utilice el mandato **wrap** para realizar una prueba de datos de bucle de retorno en la interfaz ATM del adaptador. El mandato wrap se puede emitir por VC especificando pares de VPI-VCI. Los datos repiten el bucle de retorno internamente.

Puede iniciar un reinicio, detener un reinicio o visualizar los valores actuales del reinicio selectivamente.

Si detiene o visualiza un reinicio, se visualizarán las estadísticas siguientes:

- Transmisiones de reinicio
- Recepciones de reinicio
- Errores de transmisión de reinicio
- Errores de recepción de reinicio
- Tiempos de espera excedidos de recepción de reinicio

En la visualización, se visualizan las estadísticas de reinicio actuales.

En la detención, se visualizan las estadísticas de reinicio finales.

Sintaxis:

```
wrap                display
                    start
                    stop
```

display

Visualiza los valores de reinicio actuales.

start Inicia el procedimiento de reinicio y especifica la longitud de VPI-VCI del patrón y el patrón en sí.

Ejemplo:

```
ATM Interface+ wrap start
VPI [0]?
VCI [32]?
wrap pattern length [32]?
Enter 32-byte wrap pattern: [ABCDEFGHIJKLMN0PQRSTUVWXYZ123456]
```

stop Detiene el procedimiento de reinicio y visualiza las estadísticas finales de reinicio.

Mandatos de supervisión ATM-LLC

Esta sección explica los mandatos para supervisar la multiplexión ATM LLC.

Entre los mandatos en el indicador ATM-LLC+.

Tabla 44. Resumen de los mandatos de configuración ATM LLC

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado "Cómo obtener ayuda" en la página 10.
List	Lista varias opciones

Mandatos de supervisión ATM-LLC (Talk 5)

Tabla 44. Resumen de los mandatos de configuración ATM LLC (continuación)

Mandato	Función
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página 11.

List

Utilice el mandato **list** para listar las distintas categorías de datos de supervisión ATM LLC.

Sintaxis:

```
list                endpoints
                    channels
```

endpoints

Lista las direcciones ATM que usan los protocolos que utilizan la función de multiplexión ATM-LLC en el dispositivo. El punto final se visualiza como el Identificador del sistema final y el Selector.

Ejemplo: list endpoints

```
ATM-LLC+ list endpoints
```

channels

Lista los canales que usan los protocolos que utilizan la función de multiplexión ATM-LLC en el dispositivo.

Ejemplo: list channels

```
ATM-LLC+ list channels
```

Mandatos de supervisión de interfaz virtual ATM

La supervisión de la interfaz virtual ATM se realiza utilizando los mandatos de supervisión ATM LLC. Consulte la sección “Mandatos de supervisión ATM-LLC” en la página 327 para obtener información adicional.

Soporte para la reconfiguración dinámica de ATM y ATM virtual

Esta sección describe la reconfiguración dinámica (DR) en la medida en que afecta a los mandatos Talk 6 y Talk 5.

Delete Interface de CONFIG (Talk 6)

ATM y ATM virtual soportan el mandato **delete interface** de CONFIG (Talk 6) sin ninguna restricción.

Activate Interface de GWCON (Talk 5)

ATM y ATM virtual soportan el mandato **activate interface** de GWCON (Talk 5) con la consideración siguiente:

No puede activarse una red base ATM.

El mandato **activate interface** de GWCON (Talk 5) soporta todos los mandatos específicos de las interfaces ATM y ATM virtual.

Reset Interface de GWCON (Talk 5)

ATM y ATM virtual soportan el mandato **reset interface** de GWCON (Talk 5) con la consideración siguiente:

No puede restablecerse una red base ATM.

El mandato **reset interface** de GWCON (Talk 5) soporta todos los mandatos específicos de las interfaces ATM y ATM virtual.

Mandatos de supervisión de interfaz virtual ATM (Talk 5)

Capítulo 26. Utilización de los LAN Emulation Client

Este capítulo describe los LAN Emulation Client (LEC). Incluye las secciones siguientes:

- “Visión general de LAN Emulation Client”

Visión general de LAN Emulation Client

En el direccionador, los LEC hacen las funciones de los “puertos” o “interfaces” de los direccionadores y puentes tradicionales. El direccionador tiende puentes y direcciona el tráfico entre los puertos al recibir y transmitir el tráfico mediante sus LEC.

El LEC tiene dos niveles de indicador:

1. `LE Client Config>` le permite entrar mandatos que controlan el entorno de todos los LEC. Los mandatos de este nivel de indicador se describen en “Configuración de los clientes de emulación de LAN” en la página 333
2. Uno de los mandatos, **config**, le conduce a otro nivel de indicador, `LEC Config>`, en el que puede entrar mandatos para configurar un LEC específico.

A continuación, se ofrece una explicación de los mandatos para los clientes de emulación de LAN.

Capítulo 27. Configuración y supervisión de LAN Emulation Clients

Este capítulo describe cómo configurar LAN Emulation Clients (LEC). Incluye las secciones siguientes:

- “Configuración de los clientes de emulación de LAN”
- “Configuración de un LE Client conforme a ATM Forum” en la página 334
- “Acceso al entorno de supervisión del LEC” en la página 353
- “Mandatos de supervisión del LEC” en la página 353
- “Soporte para la reconfiguración dinámica de LEC” en la página 364

Configuración de los clientes de emulación de LAN

Esta sección presenta un resumen y una explicación de los mandatos para configurar y utilizar el conjunto de clientes LE Client de una interfaz ATM en particular.

Para obtener el indicador `LE Client Config>`, entre **le-c** en el indicador `ATM Config>`, tal como se describe en “Mandatos de configuración ATM” en la página 315.

Entre los mandatos en el indicador `LE Client Config>` bajo el indicador `ATM Config>`, tal como se describe en “Mandatos de configuración ATM” en la página 315.

Tabla 45. Resumen de los mandatos de configuración de LAN EMULATION Client

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página 10.
Add	Añade un LEC para los siguientes tipos de arquitecturas de LAN emuladas que se ajustan al ATM Forum: <ul style="list-style-type: none">• Ethernet• Red en Anillo
Config	Le conduce al indicador <code>LEC Config></code> , desde el cual puede configurar un LAN Emulation Client específico.
List	Lista los LEC.
Remove	Elimina un LEC.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página 11.

Add

Utilice el mandato **add** con el fin de añadir un LEC para una LAN emulada de Red en Anillo o Ethernet.

Sintaxis:

```
add Ethernet  
Token Ring
```

token-ring

LAN emulada de Red en Anillo

Ejemplo: `add token ring`

LE Client Config>

```
LE Client Config> add token-ring  
Added Emulated LAN as interface 3
```

ethernet

LAN emulada Ethernet

Ejemplo: add ethernet

```
LE Client Config> add ethernet  
Added Emulated LAN as interface 2
```

Config

Utilice el mandato **config** para obtener el indicador LE Client Config>, desde el cual puede configurar los detalles de un LAN Emulation Client específico.

Sintaxis:

config núm. interfaz

núm. interfaz

Número entero asignado por el direccionador cuando se ha añadido el LEC a la configuración. Utilice el mandato **list** para determinar el número de interfaz asignado al LEC.

Ejemplo: config

```
LE Client Config> config 3  
ATM LAN Emulation Client configuration
```

List

Utilice el mandato **list** para listar los clientes de emulación de LAN.

Sintaxis:

list

Ejemplo:

```
LE Client Config> list  
                          ATM Forum Compliant Emulated LANs  
-----  
Physical ATM interface number = 0  
LEC interface number = 1  
Emulated LAN type     = Token Ring Forum Compliant  
Emulated LAN name     =
```

Remove

Utilice el mandato **remove** para eliminar un LEC. Debe especificar el número de interfaz que se ha asignado cuando se ha añadido el LEC a la configuración. Utilice el mandato **list** para determinar el número de interfaz asignado al LEC.

Sintaxis:

remove núm. interfaz

núm. interfaz

Número entero asignado por el direccionador.

Configuración de un LE Client conforme a ATM Forum

Utilice este proceso para acceder al indicador LE Client Config> adecuado:

1. Utilice el mandato **config** en el indicador LE Client Config> para acceder al número de interfaz LEC adecuado o utilice el mandato de configuración **network** con el número adecuado de interfaz LEC.

Configuración de Forum LE Clients

2. Entre los mandatos adecuados en el indicador Ethernet Forum Compliant LEC Config> o en el indicador Token Ring Forum Compliant LEC Config>. Los mandatos de la tabla siguiente se aplican a los LEC de Red en Anillo y Ethernet excepto los indicados.

Esta sección explica los mandatos para configurar un LAN Emulation Client conforme a ATM Forum.

Tabla 46. Resumen de los mandatos de configuración de LAN Emulation Client

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página 10.
ARP-Configuration	Le permite configurar la configuración LE-ARP para el cliente conforme a ATM Forum.
Frame	Establece el tipo de encapsulación IPX de NetWare.
IP-Encapsulation	Establece la encapsulación IP como Ethernet (tipo X'0800') o IEEE (802.3 con SNAP). Sólo se aplica a los LEC Ethernet.
List	Lista la configuración del LAN Emulation Client.
LLC	Accede al indicador de configuración LLC Config> para los LEC de Red en Anillo.
QoS-Configuration	Le lleva al indicador e1an-x LEC QoS Config> desde el cual puede configurar la Calidad de los servicios, tal como se describe en la sección LE Client QoS Configuration Commands de la publicación <i>Utilización y configuración de las características</i> .
RIF-Timer	Establece la cantidad máxima de tiempo que se conserva la información del RIF antes de renovarse. Sólo se aplica a los LEC de Red en Anillo.
Set	Establece los parámetros de LAN Emulation Client.
Source-routing	Se utiliza para habilitar o inhabilitar el puente de direccionamiento de origen. Sólo se aplica a los LEC de Red en Anillo.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página 11.

ARP Configuration

Utilice el mandato **arp-configuration** para configurar las entradas LE-ARP estáticas para el LAN Emulation Client conforme a ATM Forum.

Sintaxis:

arp-configuration

Ejemplo:

```
Token Ring Forum Compliant LEC Config> arp-configuration
ATM LAN Emulation Clients ARP configuration
```

Tabla 47. Resumen de los mandatos ARP Configuration de ATM LAN Emulation Client

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página 10.

Configuración de Forum LE Clients

Tabla 47. Resumen de los mandatos ARP Configuration de ATM LAN Emulation Client (continuación)

Mandato	Función
Add	Añade una entrada de antememoria LE-ARP utilizando un MAC o un ARP de descriptor de ruta.
Config	Establece los valores de parámetros QoS de entrada de antememoria.
List	Lista las entradas de antememoria ARP configuradas.
Remove	Elimina una entrada de antememoria ARP.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página 11.

Add

Utilice el mandato **add** para añadir una entrada de antememoria ARP utilizando la dirección MAC o un descriptor de ruta.

Las direcciones MAC y los descriptors de ruta se entran como series de caracteres hexadecimales con o sin caracteres separadores opcionales entre los bytes. Los caracteres separadores válidos son guiones (-), puntos (.) o dos puntos (:).

Sintaxis:

```
add                mac
                    route-descriptor
```

Ejemplo 1:

```
ARP config for LEC>add mac
MAC address of LE ARP Entry []? 123456789098
ATM address in 00.00.00.00.00.00:... form []? 390f0000000000000000000000000000123456789098
Destination Type - REMOTE or LOCAL [Remote]?
```

Ejemplo 2:

```
ARP config for LEC>add route 12.34
ATM address in 00.00.00.00.00.00:... form []? 390f00000000000000000000000000001234567890988888
ARP config for LEC>
```

Config

Utilice el mandato **Config** para configurar los parámetros QoS de la entrada de antememoria ARP permanente para el LAN Emulation Client específico de ATM Forum.

Sintaxis:

```
config                número-entrada-arp
```

Ejemplo:

```
ARP config for LEC> config
ARP entry number [1]
Configure LEC ARP entry
```

Tabla 48. Resumen de los mandatos ARP Config de ATM LAN Emulation Client

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado "Cómo obtener ayuda" en la página 10.

Configuración de Forum LE Clients

Tabla 48. Resumen de los mandatos ARP Config de ATM LAN Emulation Client (continuación)

Mandato	Función
Set	Establece los valores de parámetros QoS.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página 11.

Set:

Utilice el mandato **Set** para configurar los parámetros QoS de la entrada de antememoria ARP permanente para el LAN Emulation Client específico de ATM Forum.

Sintaxis:

```
set                max-reserved-bandwidth
                   traffic-type
                   peak-cell-rate
                   sustained-cell-rate
                   qos-class
                   max-burst-size
```

Ejemplo:

```
ARP entry 'identificador' config> set ?
MAX-RESERVED-BANDWIDTH
TRAFFIC-TYPE
PEAK-CELL-RATE
SUSTAINED-CELL-RATE
QOS-CLASS
MAX-BURST-SIZE
```

Consulte la sección Configuración y Supervisión de la Calidad de Servicio (QoS) de la publicación *Utilización y configuración de las características* para ver información detallada de los parámetros QoS.

List

Utilice el mandato **list** para visualizar información acerca de la configuración ARP.

Remove

Utilice el mandato **remove** para eliminar una dirección MAC configurada o una entrada LE-ARP de descriptor de ruta.

Seleccione el número de entrada ARP que se ha de eliminar en la lista proporcionada.

Sintaxis:

```
remove            número-entrada-arp
```

Frame

Utilice el mandato **frame** para establecer el tipo de encapsulación IPX de NetWare. Las opciones del mandato difieren dependiendo del tipo de LEC (Red en anillo o Ethernet). Para los LEC de Red en Anillo entre uno de los siguientes:

Configuración de Forum LE Clients

Opción	Descripción	Sintaxis
Red en Anillo que utiliza MSB	Utiliza la cabecera estándar de 802.2 IPX con el orden de bits de dirección de Red en Anillo no canónica (MSB).	frame token-ring msb
Red en Anillo que utiliza LSB	Utiliza la cabecera 802.2 IPX con el orden de bits de dirección canónica (LSB).	frame token-ring lsb
Red en Anillo con 802.2 SNAP que utiliza MSB	Utiliza el formato 802.2 con una cabecera SNAP y el orden de bits de dirección no canónica. Esta encapsulación se utiliza principalmente en entornos de puente.	frame token-ring_snap msb
Red en Anillo con 802.2 SNAP que utiliza LSB	Utiliza el formato 802.2 con una cabecera SNAP y el orden de bits de dirección canónica.	frame token-ring_snap lsb
Ethernet 2.0	Utiliza el protocolo 81-37 de Ethernet versión 2.0.	frame ethernet_II
Ethernet 802.2	Utiliza Ethernet 802.3 con 802.2 SA E0.	frame ethernet_8022
Ethernet 802.3	Utiliza Ethernet 802.3 sin ninguna cabecera 802.2.	frame ethernet_802.3
Ethernet SNAP	Utiliza 802.3, 802.2 con SNAP PID 00-00-00-81-37.	frame ethernet_SNAP

Sintaxis:

frame *tipo-encapsulación-ipx*

Nota: El mandato frame no se puede utilizar en el proceso de configuración de la red para establecer la encapsulación IPX a menos que la interfaz se haya configurado con IPX.

La encapsulación IPX también puede establecerse en el entorno de configuración IPX. Consulte el capítulo titulado "Configuración y supervisión de IPX" de la publicación *Consulta de configuración y supervisión de protocolos* para ver los detalles.

Ejemplo:

```
frame token_ring msb
```

IP-Encapsulation (sólo para los LEC Ethernet conformes a ATM Forum)

Utilice el mandato **IP-encapsulation** para seleccionar Ethernet (Ethernet tipo X'0800'), IEEE 802.3 (Ethernet 802.3 con SNAP) o ambos.

La opción **both** permite que el 2216 utilice la encapsulación Ethernet para transmitir a los sistemas principales que tienen encapsulación Ethernet y utilizar la encapsulación IEEE 802.3 para transmitir a los sistemas principales que tienen encapsulación IEEE 802.3. Si la LAN Ethernet incluye unos sistemas principales que utilizan un tipo de encapsulación y otros que utilizan el otro, si se entra **both** permite que todos ellos se comuniquen.

La opción **both** sólo se aplica a las tramas de vertimiento único. Si entra **both**, se le solicita que entre **ethernet** o **ieee-802.3** para las tramas de difusión o de multidifusión.

Sintaxis:

IP-encapsulation

- ethernet
- ieee-802.3
- both

Ejemplo:

```
Ethernet Forum Compliant LEC Config> ip-encapsulation both  
How would you like IP broadcast/multicast frames to be sent (ETHER/IEEE-802.3) [ETHER]?
```

List

Utilice el mandato **list** para listar la configuración del cliente LE.

Sintaxis:

list

LLC

Se puede decir que el Control de enlace lógico es un “subprotocolo”. No se accede directamente desde el entorno Talk 6 (configuración) ni desde el entorno Talk 5 (consola). En su lugar, se accede desde el menú de configuración del LEC de Red en Anillo, entrando un mandato **LLC**.

Utilice el mandato **llc** para acceder al indicador LLC Config>. Consulte la sección “Mandatos de configuración LLC” en la página 351 para obtener más información.

Sintaxis:

llc

QoS

Utilice el mandato **qos-configuration** para ir al indicador LEC QoS Config> desde el cual puede configurar la Calidad de los servicios, tal como se describe en la sección Mandatos de configuración de LE Client QoS de la publicación *Utilización y configuración de las características*.

Sintaxis:

qos-configuration

RIF-Timer (sólo para los LEC conformes a Token-Ring Forum)

Utilice el mandato **RIF-Timer** para establecer la cantidad máxima de tiempo que se conserva la información del RIF antes de renovarse. El rango es de 0 a 4096. El valor por omisión es de 120 segundos.

Sintaxis:

rif-timer *valor*

Ejemplo:

```
rif-timer 100
```

Configuración de Forum LE Clients

Set

Utilice el mandato **set** para establecer los parámetros de LE Client.

Sintaxis:

set arp-aging-time
arp-cache-size
arp-queue-depth
arp-response-time
auto-config
best-effort-peakrate
bus-connect-retries
conn-completion-time
control-timeout
data-direct-timeout
data-direct-vcc-mode
elan-name
esi-address
flush-timeout
forward-delay
forward-disconnect-timeout
frame-size
initial-control-timeout
lecs-atm-address
les-atm-address
mac-address
multicast-send-avg
multicast-send-peak
multicast-send-type
multiplier-control-timeout
path-switch-delay
reconfig-delay-min
reconfig-delay-max
retry-count
selector
trace
unknown-count
unknown-time
vcc-timeout

arp-aging-time

Establece el tiempo de antigüedad de ARP. Se trata del tiempo máximo que un LEC conservará una entrada en su antememoria LE_ARP en ausencia de verificación de esa relación. Un tiempo de antigüedad mayor puede dar como resultado un tiempo de configuración de sesión más rápido, pero también puede utilizar más memoria y reacciona más lentamente a los cambios en la configuración de la red.

Valores válidos:

Un número entero de segundos en el rango de 10 a 300.

Valor por omisión:

300

Ejemplo:

```
LEC Config> set arp-aging-time 200
```

arp-cache-size

Establece el número de entradas en la antememoria ARP. El tamaño de la antememoria ARP limita el número de VCC de datos directos simultáneas. Las antememorias ARP mayores necesitan más memoria, pero permiten que el cliente converse simultáneamente con un número mayor de destinos.

Valores válidos:

Un número entero en el rango de 10 a 65535.

Valor por omisión:

5000

Ejemplo:

```
LEC Config> set arp-cache-size 10
```

arp-queue-depth

Establece el número máximo de tramas en cola por entrada de antememoria ARP. Las tramas puestas en cola del LEC cuando se conmuta la vía de acceso de datos desde la VCC de envío de multidifusión a una VCC de datos directos. Se eliminarán las tramas pasadas al LEC para transmisión si la cola está llena. Una cola mayor necesita más memoria, pero da como resultado la eliminación de menos tramas durante la conmutación de vías de acceso de datos.

Valores válidos:

Un número entero en el rango de 0 a 10.

Valor por omisión:

5

Ejemplo:

```
LEC Config> set arp-queue-depth 10
```

arp-response-time

Establece el tiempo de respuesta ARP esperado. Este valor controla la frecuencia con la que se reintenta una petición ARP del LE sin responder. Los valores mayores dan como resultado menos ARP del LE, lo que causa menos tráfico y posiblemente aumenta el tiempo para establecer una VCC de datos directos.

Valores válidos:

Un número entero de segundos en el rango de 1 a 30.

Configuración de Forum LE Clients

Valor por omisión:

1 segundo

Ejemplo:

```
LEC Config> set arp-response-time 20
```

auto-config

Especifica si este LEC utiliza la modalidad de configuración automática del LECS. Especifique YES o NO. El LEC puede ponerse en contacto con el LECS para obtener la dirección de su LES y otros parámetros de configuración.

Valores válidos:

Si es YES, no tiene que configurar la dirección ATM del LES.

Si es NO, *debe* configurar la dirección ATM del LES utilizando el mandato **set les-atm-address**, tal como se describe en la página 345.

Valor por omisión:

NO

Ejemplo:

```
LEC Config> set auto-config yes
```

best-effort-peakrate

Establece la Velocidad de pico de mejor esfuerzo. Se utiliza cuando se establecen conexiones de envío de multidifusión del mejor esfuerzo.

La velocidad de pico máximo depende de la velocidad máxima de datos del dispositivo ATM.

Especifique un entero del 1 a la velocidad máxima de pico en kbps (la definición es la velocidad máxima de datos) de la manera siguiente:

- Si la velocidad máxima de datos ATM es 25 Mbps, la velocidad máxima de pico es 25.000 kbps.
- Si la velocidad máxima de datos ATM es 155 Mbps, la velocidad máxima de pico es 155.000 kbps.

Valores válidos:

Un número entero en el rango de 1 a la velocidad máxima de datos de dispositivo.

Valor por omisión:

155000

Ejemplo:

```
LEC Config> set best-effort-peakrate 24000
```

bus-connect-retries

Este parámetro establece el número máximo de veces que el LEC intentará volver a conectarse al BUS antes de volver al estado inicial.

Valores válidos:

De 0 a 2

Valor por omisión:

1

connection-completion-time

Establece el tiempo de terminación de conexión. Este es el intervalo de tiempo en el cual se esperan datos o un mensaje READY_IND de una parte llamadora.

Cuando se establece una VCC de datos directos para el cliente, el LEC espera datos o un mensaje READY_IND dentro de este período de tiempo. El LEC no transmitirá tramas a través de una VCC de datos directos establecida con el hasta la recepción de datos o de READY_IND. Este valor de parámetro controla el período de tiempo que pasa antes de que el LEC emita un READY QUERY (en saltos de recepción de un READY_IND). Los valores inferiores conducen a tiempos de respuesta más rápidos, pero también a transmisiones innecesarias.

Valores válidos:

Un número entero de segundos en el rango de 1 a 10.

Valor por omisión:

4

Ejemplo:

```
LEC Config> set connection-completion-time 5
```

control-timeout

Este parámetro establece el tiempo de espera de control acumulado máximo de una petición.

Un valor de tiempo de espera actual se inicializa al valor de *initial-control-timeout*. Si no se recibe una respuesta a una petición dentro del valor de tiempo de espera actual, el tiempo de espera actual se multiplica por el valor de *multiplier-control-timeout* y se vuelve a emitir la petición. Cada vez que caduca el valor de tiempo de espera actual, se repite este proceso hasta que el valor actual de tiempo de espera excede el valor de *control-timeout*.

Valores válidos:

Un número entero de segundos en el rango de 10 a 300.

Valor por omisión:

30

Ejemplo:

```
LEC Config> set control-timeout 100
```

data-direct-timeout

Especifica el valor de tiempo de espera para la VCC de datos directos. Este parámetro limita el tiempo que las VCC de datos directos se dejan activas sin que el LEC tenga una conexión con el LES/BUS. Si el LEC se vuelve a unir a un LES/BUS antes de que caduque el temporizador, el tiempo se detiene.

Valores válidos:

De 10 a 300 segundos

Valor por omisión:

30

data-direct-vcc-mode

Especifica si la modalidad de VCC de datos directos persistente está habilitada o inhabilitada. Cuando la modalidad de VCC de datos directos está habilitada, si el LEC pierde su conexión con el LES/BUS, las VCC de

Configuración de Forum LE Clients

datos directos no se eliminan y se inicia el temporizador de tiempo de espera de reconexión. El LEC continuará intentando volverse a conectar al LES/BUS. Si el LEC no puede volverse a conectar al LES/BUS antes de que caduque el **data-direct-timeout**, se desconectarán todas las VCC de datos directos.

Valores válidos:

yes o no

Valor por omisión:

no

elan-name

Especifica el nombre de la ELAN a la que el LEC desea unirse. Se trata del nombre de ELAN enviado al LECS en la petición de configuración (si el LEC se configura automáticamente) o al LES en la petición de unión. El LECS o LES puede devolver un nombre de ELAN distinto en la respuesta.

Valores válidos:

Cualquier serie de caracteres de 0 a 32 bytes de longitud.

Valor por omisión:

En blanco

Nota: Un nombre en blanco (serie de longitud 0) es válido.

Ejemplo:

```
LEC Config> set elan-name FUZZY
```

esi-address

Establece la parte del ESI de la dirección ATM del LEC.

Especifique la parte del ESI (octetos 13 a 19) de la dirección ATM del LEC. La combinación de ESI y selector del LEC debe ser exclusiva entre todos los componentes de LAN Emulation del dispositivo.

Valores válidos:

Cualquier combinación de 12 dígitos hexadecimales.

Valor por omisión:

ESI incorporado

Ejemplo:

```
set esi
Select ESI
(1) Use burned in ESI
(2) 11.22.33.44.55.66

Enter selection [1]?
```

flush-timeout

Establece el tiempo de espera de vaciado. Se trata del tiempo límite que se ha de esperar para recibir la respuesta LE_FLUSH_RESPONSE después de que se haya enviado petición LE_FLUSH_REQUEST antes de la acción de recuperación. Durante la recuperación, se eliminan las tramas en cola y se envía una nueva petición de vaciado.

Cuando se conmuta desde el envío de multidifusión a una vía de acceso de datos directos, el cliente envía una petición de vaciado de la VCC de envío de multidifusión. Hasta que se reciba la respuesta de vaciado o hasta que caduque el retardo del conmutador de vía de acceso, las tramas se ponen en cola para el destino.

Valores válidos:

Un número entero de segundos en el rango de 1 a 4.

Valor por omisión:

4

Ejemplo:

```
LEC Config> set flush-timeout 3
```

forward-delay

Establece el retardo de reenvío. Las entradas en la antememoria ARP deben volverse a verificar periódicamente. El tiempo de retardo de reenvío es el período de tiempo máximo que una entrada remota puede permanecer en la antememoria durante un cambio de topología de la red. Los tiempos de antigüedad más largos pueden dar como resultado entradas antiguas (no válidas), pero también pueden causar menos tráfico de vuelta a verificar.

Valores válidos:

Un número entero de segundos en el rango de 4 a 30.

Valor por omisión:

15

Ejemplo:

```
LEC Config> set forward-delay 10
```

forward-disconnect-timeout

Este parámetro establece el período de tiempo que un LEC esperará después de perder su última VCC de reenvío de multidifusión desde el BUS antes de volver al estado inicial. Este retraso permite que el BUS intente volver a conectarse con el cliente sin volver al estado inicial.

Valores válidos:

De 10 a 300 segundos

Valor por omisión:

60

frame-size

Establece el tamaño de trama.

El valor especificado para frame-size debe ser igual o inferior al valor especificado para el max-frame ATM utilizando el mandato ATM INTERFACE> set max-frame tal como se describe en la página 319.

Valores válidos:

1516

4544

9234

18190

Valor por omisión:

Si el tipo de ELAN es de Red en anillo, el valor por omisión es 4544. Si el tipo de ELAN es Ethernet, el valor por omisión es 1516.

Ejemplo:

```
LEC Config> set frame-size 4544
```

Configuración de Forum LE Clients

initial-control-timeout

Este parámetro establece el valor del tiempo de espera de control inicial utilizado en el algoritmo de tiempo de espera de control descrito en 343.

Valores válidos:

De 1 a 10

Valor por omisión:

5

Ejemplo:

```
LEC Config> set initial-control-timeout 10
```

lecs-atm-address

Especifica la dirección ATM del LECS.

Si el cliente se establece en configuración automática, intenta conectarse a un LECS. Si no puede conectarse a un LECS, puede intentar otra dirección ATM del LECS. Las direcciones ATM del LECS que se han intentado por orden, son:

1. Esta dirección LECS configurada
2. Cualquier dirección LECS obtenida a través de ILMI
3. La dirección LECS bien conocida definida por ATM Forum.

No se proporciona ningún valor por omisión.

Nota: Este mandato debe entrarse en una línea de mandatos. Aquí aparece en dos líneas debido a problemas de espacio.

Ejemplo:

```
LEC Config> set lecs-atm-address  
39.84.0F.00.00.00.00.00.00.00.01.10.00.5A.00.DE.AD.01
```

les-atm-address

Establece la dirección ATM del LES. Este mandato puede ser opcional o necesario dependiendo del valor de lecs-auto-config, tal como se describe en el mandato **set auto-config** en la página 342.

- Si auto-config es YES, les-atm-address no es configurable.
- Si auto-config es NO, les-atm-address es necesario.

Especifique la dirección ATM del LES. No se proporciona ningún valor por omisión.

Nota: Este mandato debe entrarse en una línea de mandatos. Aquí aparece en dos líneas debido a problemas de espacio.

Ejemplo:

```
LEC Config> set les-atm-address  
39.84.0F.00.00.00.00.00.00.00.01.10.00.5A.00.DE.AD.02
```

mac-address

Establece la dirección MAC para este cliente LE. *Puede* especificar que el cliente utilice la dirección MAC incorporada de la interfaz ATM o puede especificar una dirección MAC diferente. Si tiene dos clientes que tienen un puente entre ellos, deben utilizar direcciones MAC diferentes.

Si tiene dos clientes y cada uno tiene configurado IPv6, estos clientes deben utilizar direcciones MAC diferentes.

Esta dirección MAC se registra en el LES cuando el cliente se une a la ELAN.

Valores válidos:

Cualquier dirección MAC válida.

Valor por omisión:

ninguno

Ejemplo:

```
LEC Config> set mac-address
Use adapter address for MAC? [No]
MAC address []: 10.00.5a.00.00.01
```

multicast-send-avg

Establece la velocidad promedio de VCC de envío de multidifusión en kbps. Lo utiliza el LEC para reservar ancho de banda de la VCC para el BUS. Especifica la velocidad de célula sostenida hacia adelante y hacia atrás utilizada durante la configuración de una VCC de envío de multidifusión de ancho de banda reservado.

Este parámetro sólo se puede aplicar cuando multicast-send-type es de ancho de banda reservado. Si multicast-send-avg es igual a multicast-send-peak, se señala un envío de multidifusión de velocidad constante de bits (CBR). De lo contrario, se señala un envío de multidifusión de velocidad variable de bits (VBR). Multicast-send-avg debe ser inferior o igual a multicast-send peak.

Una VCC de envío de multidifusión de ancho de banda reservado puede mejorar las velocidades de transferencia de datos de las redes congestionadas, pero si se reserva el ancho de banda y no se utiliza se malgastan recursos de red.

Cuando multicast-send-type está reservado, deben especificarse multicast-send-avg y multicast-send-peak.

Ejemplo:

```
LEC Config> set multicast-send-avg 4000
```

multicast-send-peak

Establece la velocidad de pico de envío de multidifusión en kbps. Se utiliza por el LEC para reservar el ancho de banda de la VCC para el BUS. Especifica la velocidad de célula de pico de hacia adelante y hacia atrás utilizada al establecer una VCC de envío de multidifusión de ancho de banda reservado.

Este parámetro sólo se puede aplicar cuando multicast-send-type es de ancho de banda reservado. Si multicast-send-avg es igual a multicast-send-peak, se señala un envío de multidifusión de velocidad constante de bits (CBR). De lo contrario, se señala un envío de multidifusión de velocidad variable de bits (VBR). Multicast-send-avg debe ser inferior o igual a multicast-send peak.

Una VCC de envío de multidifusión de ancho de banda reservado puede mejorar las velocidades de transferencia de datos de las redes congestionadas, pero si se reserva el ancho de banda y no se utiliza se malgastan recursos de red.

Cuando multicast-send-type está reservado, deben especificarse multicast-send-avg y multicast-send-peak.

Ejemplo:

```
LEC Config> set multicast-send-peak 155
```

Configuración de Forum LE Clients

multicast-send-type

Establece el tipo de envío de multidifusión. Especifica el método utilizado por el LEC al establecer la VCC de envío de multidifusión.

Si `multicast-send-avg` es igual a `multicast-send-peak`, se señala un envío de multidifusión de velocidad constante de bits (CBR). De lo contrario, se señala un envío de multidifusión de velocidad variable de bits (VBR). `multicast-send-avg` debe ser como mínimo igual a `multicast-send-peak`.

Una VCC de envío de multidifusión de ancho de banda reservado puede mejorar las velocidades de transferencia de datos de las redes congestionadas, pero si se reserva el ancho de banda y no se utiliza se malgastan recursos de red.

Cuando el tipo `multicast-send-type` es reservado, deben especificarse `multicast-send-no` y `multicast-send-peak`.

Valores válidos:

Mejor esfuerzo o reservado

Valor por omisión:

Mejor esfuerzo

Ejemplo:

```
LEC Config> set multicast-send-type best-effort
```

multiplier-control-timeout

Este parámetro establece el valor del multiplicador de tiempo de espera de control utilizado en el algoritmo de tiempo de espera de control descrito en la página 343.

Valores válidos:

De 2 a 5

Valor por omisión:

2

Ejemplo:

```
LEC Config> set multiplier-control-timeout 5
```

path-switch-delay

Establece el retardo del conmutador de vía de acceso.

El LEC debe asegurarse de que todas las tramas enviadas a través del BUS a un destino hayan llegado al destino antes de que pueda empezar a utilizar una VCC de datos directos. Esto se hace utilizando el protocolo de vaciado o esperando `path-switch-delay` segundos después de enviar el último paquete al BUS. Los valores menores mejoran el rendimiento, pero pueden dar como resultado paquetes fuera de secuencia en una red muy congestionada.

Valores válidos:

Un número entero de segundos en el rango de 1 a 8.

Valor por omisión:

6

Ejemplo:

```
LEC Config> set path-switch-delay 5
```

reconfig-delay-min

Este parámetro establece el tiempo de retardo mínimo cuando el LEC vuelve al estado inicial. Este valor debe ser \leq *reconfig-delay-max*.

Valores válidos:

De 1 al valor de *reconfig-delay-max*

Valor por omisión:

1

Ejemplo:

```
LEC Config> set reconfig-delay-min 5
```

reconfig-delay-max

Este parámetro establece el tiempo máximo de retardo cuando el LEC vuelve al estado inicial. Este valor debe ser \geq *reconfig-delay-min*.

Valores válidos:

De 1 a 10

Valor por omisión:

5

Ejemplo:

```
LEC Config> set reconfig-delay-max 9
```

retry-count

Establece la cuenta de reintentos. Es el número máximo de veces que el LEC reintenta una petición LE_ARP_REQUEST para un destino LAN de una trama específica. Si no se recibe ninguna respuesta ARP después del número de reintentos especificados, la entrada se depura de la antememoria ARP del LE.

Valores válidos:

0, 1 ó 2

Valor por omisión:

1

Ejemplo:

```
LEC Config> set retry-count 2
```

selector

Especifica la parte del selector de la dirección ATM del cliente. La combinación de ESI y selector debe ser exclusiva entre todos los componentes LANE del dispositivo. Por omisión, se selecciona un selector exclusivo para el ESI configurado.

Valores válidos:

Cualquier octeto, en hexadecimal, que otro componente LANE con el mismo ESI no utilice.

Ejemplo:

```
LEC Config> set selector 01
```

trace Habilita el rastreo para el LEC. Para realizar el rastreo de paquetes, se necesitan tres pasos:

1. Habilitar el sistema de rastreo de paquetes (bajo ELS)
2. Habilitar el rastreo en el subsistema LEC (bajo ELS)
3. Habilitar el rastreo de paquetes en los LEC deseados (utilizando este mandato).

Configuración de Forum LE Clients

Valores válidos:

Yes o No

Valor por omisión:

No

Ejemplo:

```
Token Ring LEC config>set trace
Trace packets on the LEC? [No]?yes
```

unknown-count

Establece la cuenta de tramas desconocidas. Es el número máximo de tramas para una dirección MAC de vertimiento único o descriptor de ruta específicos que pueden enviarse al BUS dentro del tiempo especificado por el parámetro unknown-time. Los valores mayores reducen el número de tramas eliminadas mientras que incrementan la carga del BUS.

Valores válidos:

Un número entero de tramas del rango de 1 a 255.

Valor por omisión:

10

unknown-time

Establece el tiempo de trama desconocida. Se trata del intervalo de tiempo durante el cual pueden enviarse el número máximo de tramas para una dirección MAC de vertimiento única o un descriptor de ruta (especificado por el parámetro unknown-count) al BUS. Los valores mayores aumentan el número de tramas eliminadas mientras que reducen la carga del BUS.

Valores válidos:

Un número entero de segundos en el rango de 1 a 60.

Valor por omisión:

1

Ejemplo:

```
LEC Config> set unknown-time 5
```

vcc-timeout

Establece el tiempo de espera de la VCC. Deben liberarse las VCC de datos directos en las que no se han enviado datos durante este período de tiempo.

Valores válidos: De 0 a 31536000 segundos (1 año).

Valor por omisión: 1200

Nota: Este parámetro sólo tiene significado para conexiones SVC.

Ejemplo:

```
LEC Config> set vcc-timeout 1000
```

Source-Routing (sólo para los LEC conformes a Token-Ring Forum)

Utilice el mandato **source-routing** para habilitar o inhabilitar el direccionamiento de origen de la estación final. El direccionamiento de origen es el proceso por el cual las estaciones finales determinan la ruta de origen que se ha de utilizar para cruzar puentes de direccionamiento de origen. El direccionamiento de origen permite que los protocolos IP, IPX y AppleTalk Phase 2 lleguen a los nodos del otro lado del puente de ruta de origen.

Configuración de Forum LE Clients

Esta función del dispositivo no se cambia si se habilita o inhabilita el direccionamiento. El valor por omisión es habilitado.

Algunas estaciones no reciben correctamente las tramas con un RIF de direccionamiento de origen en ellas. Esto es especialmente común entre controladores NetWare. La inhabilitación del direccionamiento de origen en esta situación le permitirá comunicarse con estas estaciones.

El direccionamiento de origen sólo debe habilitarse si hay puentes de direccionamiento de origen en este anillo a través de los cuales desea realizar puentes de los paquetes de IP, IPX y AppleTalk Phase 2. El direccionamiento de origen también debe habilitarse para que puedan devolverse los mensajes de respuesta de prueba LLC.

Sintaxis:

```
source-routing          _enable
                           _disable
```

Ejemplo:

```
source-routing disable
```

Mandatos de configuración LLC

Esta sección resume y explica todos los mandatos LLC. Estos mandatos, que aparecen en la Tabla 49, le permiten supervisar el LLC mientras pasa paquetes a través de una red SNA.

Tabla 49. Resumen de los mandatos LLC

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado "Cómo obtener ayuda" en la página 10.
List	Visualiza información de configuración.
Set	Permite al usuario configurar dinámicamente los parámetros LLC que son válidos para la vida de la sesión.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página 11.

List

Utilice el mandato **list** para visualizar la información de configuración.

Sintaxis:

```
list
```

Set

Utilice el mandato **set** para configurar dinámicamente los parámetros LLC de una sesión LLC actual. Cualquier cambio que realice en los parámetros surtirá efecto para la vida de la sesión.

Atención: El cambio de los parámetros LLC desde los valores por omisión puede afectar a la forma en que funciona el protocolo LLC.

Configuración de LLC

Sintaxis:

set *n2-max_retry cuenta*
n3-frames-rcvd-before-ack cuenta
nw-acks-to-inc-ww cuenta
rw-receive-window segundos
t1-reply-timer segundos
t2-receive-ack-timer segundos
ti-inactivity-timer segundos
tw-transmit-window segundos

n2-max_retry

El número máximo de reintentos del protocolo LLC. Por ejemplo, N2 es el número máximo de veces que el LLC transmite un RR sin recibir un reconocimiento cuando caduca el temporizador de inactividad. El valor por omisión es 8. El mínimo es 1. El máximo es 127.

n3-frames-rcvd-before-ack

Este valor se utiliza con el temporizador T2 para reducir el tráfico de reconocimiento para las tramas I recibidas. Establezca este contador en un valor especificado. Cada vez que se recibe una trama I, se reduce este valor. Cuando este contador llega a 0 o caduca el temporizador T2, se envía un reconocimiento. El valor por omisión es 1. El mínimo es 1. El máximo es 255.

nw-acks-to-inc-ww

Este campo se establece en el valor por omisión 1.

rw-receive-window

Establece el número de tramas I que se pueden recibir antes de transmitir un RR. El valor por omisión es 2. El mínimo es 1. El máximo es 127.

t1-reply-timer

Este temporizador caduca cuando LLC no puede recibir un reconocimiento o una respuesta necesarios de otra estación LLC. Cuando caduca este temporizador, se envía un RR con el bit de sondeo establecido y se vuelve a iniciar T1. Si el LLC no recibe ninguna respuesta después del número máximo de reintentos configurados (N2), el enlace subyacente se declara no operativo. El valor por omisión es 1. El mínimo es 1. El máximo es 256.

t2-receive-ack-timer

Este temporizador se utiliza para retrasar el envío de un reconocimiento para una trama recibida en formato I. Este temporizador se inicia cuando se recibe una trama I y se restablece cuando se envía un reconocimiento. Si este temporizador caduca, LLC2 envía un reconocimiento lo antes posible. Establezca este valor de modo que sea inferior al de T1. Esto asegura que el similar LLC2 remoto recibe el reconocimiento retrasado antes de que caduque el temporizador T1. El valor por omisión es 1 (100 ms). El mínimo es 1. El máximo es 2560.

Nota: Si este temporizador se establece en 1 (el valor por omisión) no se ejecutará (por ejemplo, **n3-frames-rcvd-before-ack=1**).

ti-inactivity-timer

Este temporizador caduca cuando LLC no recibe ninguna trama durante un período de tiempo especificado. Cuando este temporizador caduca, el LLC

transmite un RR hasta que otro LLC responde o el temporizador N2 caduca. El valor por omisión es de 30 segundos. El mínimo es 1 segundo. El máximo es 256 segundos.

tw-transmit-window

Establece el número máximo de tramas I que pueden enviarse antes de recibir un RR. Suponiendo que el otro extremo de la sesión LLC pueda realmente recibir esta cantidad de tramas I consecutivas y que el dispositivo tenga suficiente memoria de almacenamiento dinámico para conservar estas copias hasta que se reciba un reconocimiento, si se incrementa este valor puede aumentarse la productividad. El valor por omisión es 2. El mínimo es 1. El máximo es 127.

Acceso al entorno de supervisión del LEC

Utilice el procedimiento siguiente para acceder a los mandatos de supervisión LEC. Este proceso le proporciona acceso al proceso de *supervisión* de LEC.

1. En el indicador OPCON, entre **talk 5**. (Para ver los detalles de este mandato consulte la sección “¿Qué es el proceso OPCON?” en la página 33.) Por ejemplo:

```
* talk 5 +
```

Después de entrar el mandato **talk 5**, se visualiza el indicador GWCON (+) en la consola. Si no aparece el indicador cuando entra en la configuración, pulse **Intro** de nuevo.

2. En el indicador +, entre el mandato **network ?** para visualizar los números de las interfaces de red para las que el dispositivo está configurado actualmente y entre el *número de interfaz* para el LEC que desea supervisar. Por ejemplo:

```
+ network ?
```

```
1 : ATM Ethernet LAN Emulation: ETH
2 : IP Protocol Network
3 : Bridge Application
5 : CHARM ATM Adapter
Network number [0]? 1
LEC+
```

Se visualiza el indicador de supervisión del LEC (LEC+).

Si conoce el número de interfaz del LEC que desea supervisar, entre el mandato **network** seguido del *número de interfaz* del LEC.

```
+ network 1
LEC+
```

Mandatos de supervisión del LEC

Esta sección resume y explica los mandatos de supervisión del LEC. Puede acceder a los mandatos de supervisión del LEC en el indicador LEC+. La Tabla 50 muestra los mandatos.

Tabla 50. Resumen de los mandatos de supervisión de LE Client

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página 10.

Supervisión de LE Clients

Tabla 50. Resumen de los mandatos de supervisión de LE Client (continuación)

Mandato	Función
List	<p>Lista:</p> <ul style="list-style-type: none"> • La tabla de resolución de direcciones (ARP) de LEC • La configuración del LEC • La información de la VCC de datos directos • Las direcciones de grupos • La información de RIF • Las estadísticas del LEC • La tabla de VCC.
LLC	Le lleva al indicador de supervisión LLC> para los LEC de Red en Anillo.
MIB	<p>Visualiza los objetos MIB del LEC incluyendo:</p> <ul style="list-style-type: none"> • La tabla de configuración MIB del LEC • La tabla ARP MAC del LEC • La tabla de descriptores de rutas del LEC • Las tablas de VCC del LEC MIB Server • La tabla de estadísticas MIB del LEC • La tabla de estado MIB de LEC
QoS	Le lleva al indicador LEC x QoS+ desde el cual puede supervisar la Calidad de los servicios, tal como se describe en la sección Quality of Service Monitoring Commands de la publicación <i>Utilización y configuración de las características</i> .
Trace	Activa o desactiva el rastreo de paquetes o establece una dirección de rastreo o máscara de rastreo.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página 11.

List

Utilice el mandato **list** para listar la Tabla de resolución de direcciones (ART) del LEC, la configuración del LEC, la información de VCC de datos directos o las estadísticas del LEC.

Sintaxis:

```
list
    arp-table
    configuration
    data-direct-vccs
    group
    rif
    statistics
    vcc-table
```

arp Lista la Tabla de resolución de direcciones del LEC (entradas en la antememoria ARP).

Ejemplo:

```
LEC+ list arp
```

```
LEC Address Resolution (LE ARP Cache) Table
```

```
Max Table Size      = 10
Free Table Entries  = 10
Current Mac Entries = 0
Current RD Entries  = 0
Arp Aging Time     = 300
Verify Sweep Interval = 60
```

Supervisión de LE Clients

MAC Address	Remote	Conn Handle	Xmit Queue Depth	BUS Frame Count	Arp Retry Count	Aging Timer	Destination	ATM Address
40.00.00.00.00.09	False	652	0	0	0	60	39.99.99.99.99.99.	99.00.00.99.99.30.02.40.00.00.00.00.09.81

Nota: El Intervalo de intercambio siempre es una quinta parte del valor del Temporizador de antigüedad de ARP.

Max Table Size

El número total de entradas disponibles

Free Table Entries

El número de entradas libres

Current MAC Entries

Current RD Entries

Las entradas ATM del descriptor de ruta

ARP Aging Time

Tiempo para que una entrada se ponga fuera por antigüedad

Verify Sweep Interval

MAC Address

Remote

Connection Handle

Queue Depth

Xmit Frame Count

BUS Retry Count

ARP Aging Timer

Destination ATM Address

configuration

Lista la configuración del LEC.

Para Ethernet:

Ejemplo:

```
IBM LEC+ list config
      ATM IBM LEC Configuration
Physical ATM interface number = 0
LEC interface number          = 7
Primary ATM address
      ESI address              = Use burned in addr
      Selector byte            = 0x3
Emulated LAN type              = Ethernet IBM
Maximum frame size             = 1523
LE Client MAC address          = Use burned in addr
LE Server ATM address          = 00.00.00.00.00.00.00.00.00.00.00.00.00.00.00.00
Forward Peak Rate              = 155000
```

Supervisión de LE Clients

```
Backward Peak Rate          = 155000
MAC cache size              = 32
MAC cache aging period     = 60
Route Descriptor cache size = 32
Route Descriptor aging period = 60
LES Registration interval   = 60
LES Registration retry count = 3
LES keep alive count       = 10
Packet trace                = No
IP Encapsulation            = ETHER
```

Para IBM de Red en Anillo:

Ejemplo:

IBM LEC+list config

```
ATM IBM LEC Configuration
Physical ATM interface number = 0
LEC interface number         = 10
Primary ATM address
  ESI address                = Use burned in addr
  Selector byte              = 0x6
Emulated LAN type           = Token Ring IBM
Maximum frame size          = 4551
LE Client MAC address       = Use burned in addr
LE Server ATM address       = 39.84.07.00.00.00.00.00.00.00.00.00.01.10.00.5A.DD.DA.02
Forward Peak Rate           = 155000
Backward Peak Rate          = 155000
MAC cache size              = 32
MAC cache aging period     = 60
Route Descriptor cache size = 32
Route Descriptor aging period = 60
LES Registration interval   = 60
LES Registration retry count = 3
LES keep alive count       = 10
Packet trace                = No
RIF Aging Timer             = 120
Source Routing              = Enabled
```

Para conforme a Token Ring Forum:

Ejemplo:

LEC+ list config

```
Physical ATM interface number = 0
LEC interface number         = 9
LEC ATM address              = 39.99.99.99.99.99.00.00.99.99.31.01.09.FC.DD.D0.32.70.0A
LEC MAC address              = 40.00.82.10.17.09
lecConfigMode                = Manual
  lecConfigLanType           = 802.5 - Token Ring
  lecConfigMaxDataFrameSize = 4544
lecConfigLanName             =
  lecConfigLesAtmAddress     = 39.99.99.99.99.99.00.00.99.99.31.01.40.00.82.10.17.00.09
  lecControlTimeout          = 30
  lecMaxUnknownFrameCount    = 10
  lecMaxUnknownFrameTime    = 1
lecVccTimeoutPeriod          = 1200
lecMaxRetryCount             = 1
lecAgingTime                  = 300
lecForwardDelayTime          = 15
lecExpectedArpResponseTime  = 1
lecFlushTimeout              = 4
lecPathSwitchingDelay        = 6
  lecLocalSegmentId          = 0x0
lecMulticastSendType         = 1
  lecMulticastSendAvgRate    = 365566
  lecMulticastSendPeakRate   = 365566
lecConnectionCompleteTimer  = 4
lecInitialControlTimeout     = 5
  lecControlTimeoutMultiplier = 2
  V2 Capable                  = TRUE
lecForwardDisconnectTimeout  = 60
lecMinReconfigDelay          = 1
lecMaxReconfigDelay          = 5
  lecMaxBusConnectRetries    = 0
  lecElanId                   = 0
  ExplorerExclude             = TRUE
Data direct VCC mode         = TRUE
Data direct timeout          = 20
LE ARP queue depth           = 5
LE ARP cache size            = 5000
```

```

Forward peakrate      = 365566
Backward peakrate    = 365566
Packet trace         = Off
RIF aging timer      = 120
Source Routing       = enabled

```

Consulte la sección “Set” en la página 340 para ver una definición de los parámetros mostrados en los ejemplos anteriores.

data Lista la información de VCC de datos directos del LEC.

Ejemplo:

LEC+ list data

```

LEC Data Direct VCC Table

Max Table Size      = 1019      Max no of SVC connections
Current Size        = 0          Currently used
Inactivity Timeout  = 1200      No Data Xfer Timeout before connection is
                                closed (seconds)

Sweep Interval      = 60

Conn Handle  VPI  VCI  Inactive Timer  User Count  Destination ATM Address
-----
652         0  7241  300           1  39.99.99.99.99.99.00.00.99.99.30.02.
                                40.00.00.00.00.09.81
-----

```

group Lista las direcciones de los grupos que el LEC utiliza.

rif Lista la dirección MAC para las correlaciones del Campo de información de direccionamiento (RIF) que el LEC utiliza.

statistics

Lista las estadísticas del LEC.

Ejemplo:

LEC+ list stat

```

LEC Statistics

In Octets.high      = 0          No of Bytes received
In Octets.low       = 346
In Discards         = 2          Packets discarded
In Errors           = 0          Rx.Errors
In Unknown Protos  = 0          Unknown protocols received
Out Octets.high     = 0          No of Bytes xmitted.
Out Octets.low      = 0
Out Discards        = 0
Out Errors          = 0          Tx.Errors
In Frames           = 0
Out Frames          = 0
In Bytes            = 0
Out Bytes           = 0

```

VCC table

Lista la tabla VCC.

Ejemplo:

LEC+ list vcc

LLC

Se puede decir que el Control de enlace lógico es un “subprotocolo”. No se accede directamente desde el entorno Talk 6 (configuración) ni desde el entorno Talk 5 (consola). En su lugar, se accede desde el menú de supervisión del LEC de Red en Anillo entrando un mandato **LLC**.

Supervisión de LE Clients

Utilice el mandato **llc** para acceder al indicador LLC>. Consulte la sección "Mandatos de supervisión LLC" en la página 363 para obtener más información.

Sintaxis:

llc

MIB

Utilice el mandato **mib** para visualizar los objetos MIB.

Nota: Parte de esta información puede visualizarse en un formato diferente utilizando el mandato **list**.

Sintaxis:

mib config-table
mac-arp-table
rd-arp-table
server-vcc-table
statistics-table
status-table

config Visualiza la Tabla de configuración MIB del LEC.

Ejemplo:

LEC+ **mib config**

```
lecConfigTable:
lecConfigMode           = Manual
lecConfigLanType        = 802.3 - Ethernet
lecConfigMaxDataFrameSize = 1516
lecConfigLanName        =
lecConfigLesAtmAddress   = 39.84.0F.00.00.00.00.00.11.23.24.24.24.24.55.66.77.88.99.00
lecControlTimeout       = 120
lecMaxUnknownFrameCount = 1
lecMaxUnknownFrameTime  = 0
lecVccTimeoutPeriod     = 1200
lecMaxRetryCount        = 1
lecAgingTime            = 300
lecForwardDelayTime     = 15
lecExpectedArpResponseTime = 1
lecFlushTimeout         = 4
lecPathSwitchingDelay   = 6
lecLocalSegmentId       = 0
lecMulticastSendType    = 1
lecMulticastSendAvgRate = 25000000
lecMulticastSendPeakRate = 25000000

lecConnectionCompleteTimer = 4
lecInitialControlTimeout   = 5
lecControlTimeoutMultiplier= 2
lecConfigV2Capable         = TRUE
lecForwardDisconnectTimeout = 60
lecMinReconfigDelay        = 1
lecMaxReconfigDelay        = 5
lecMaxBusConnectRetries    = 1
ExplorerExclude            = FALSE
Data direct VCC mode       = TRUE
Data direct timeout        = 20
```

lecConfigMode

Modalidad de configuración del LEC: AUTO o MANUAL. Si es AUTO, el LEC utiliza el LECS para obtener la dirección ATM del LES.

lecConfigLanType

Tipo de LAN, Ethernet o Red en Anillo

lecConfigMaxDataFrameSize

Tamaño máximo de trama

lecConfigLanName

Nombre de ELAN

lecConfigLesAtmAddress

Dirección ATM del LE Server

lecControlTimeout

Tiempo excedido de espera para la trama de control de petición/respuesta

lecMaxUnknownFrameCount

Número máximo de tramas desconocidas

lecMaxUnknownFrameTime

Período en el que el LEC enviará un máximo de tramas MaxUnknownFrameCount al BUS para un Destino LAN de vertimiento único determinado y también debe iniciar el protocolo de resolución de direcciones para resolver el Destino LAN.

lecVccTimeoutPeriod

Tiempo de espera de inactividad de las VCC de datos directos de SVC

lecMaxRetryCount

Cuenta de reintentos de ARP LE

lecAgingTime

Duración de la entrada no verificada de la tabla ARP

lecForwardDelayTime**lecExpectedArpResponseTime**

Tiempo del ciclo de petición/respuesta de ARP

lecFlushTimeout

Período de tiempo de espera de Petición de vaciado/respuesta de vaciado del LE

lecPathSwitchingDelay**lecLocalSegmentId**

ID de segmento de LAN emulada. Sólo para clientes 802.5

lecMulticastSendType

Parámetro de señalización utilizado por el LEC para la VCC de envío de multidifusión

lecMulticastSendAvgRate

Parámetro de señalización utilizado por el LEC para la VCC de envío de multidifusión

lecMulticastSendPeakRate

Parámetro de señalización utilizado por el LEC para la VCC de envío de multidifusión

lecConnectionCompleteTimer

Tiempo de espera antes de enviar una consulta READY_QUERY

lecInitialControlTimeout

Especifica el tiempo de espera de control acumulado máximo

Supervisión de LE Clients

lecControlTimeoutMultiplier

Especifica el multiplicador del tiempo de espera de control

lecConfigV2Capable

Especifica si el LEC tiene la posibilidad de LANE versión 2

lecForwardDisconnectTimeout

Especifica el período de tiempo que se ha de esperar después de perder la última VCC de reenvío de multidifusión

lecMinReconfigDelay

Especifica el tiempo mínimo de retardo que el LEC espera en estado inicial

lecMaxReconfigDelay

Especifica el tiempo máximo de retardo que el LEC espera en estado inicial

lecMaxBusConnectRetries

Especifica el número máximo de reintentos de conexión al BUS antes de volver al estado inicial

ExplorerExclude

Especifica si se han de eliminar las tramas exploradoras RIF

Data Direct VCC Mode

Especifica la modalidad de datos directos persistentes

Data Direct Timeout

Especifica el tiempo de espera de la VCC de datos directos persistentes

mac Visualiza la Tabla ARP MAC del LEC

rd Visualiza la Tabla de descriptores de rutas del LEC

server Visualiza las Tablas de VCC del LEC MIB Server

Ejemplo:

LEC+ **mib server**

```
lecServerVccTable:  
  lecConfigDirectInterface    = 0  
  lecConfigDirectVpi          = 0  
  lecConfigDirectVci          = 0  
  lecControlDirectInterface   = 1  
  lecControlDirectVpi         = 0  
  lecControlDirectVci         = 38  
  lecControlDistributeInterface = 1  
  lecControlDistributeVpi     = 0  
  lecControlDistributeVci     = 37  
  lecMulticastSendInterface   = 1  
  lecMulticastSendVpi         = 0  
  lecMulticastSendVci         = 34  
  lecMulticastForwardInterface = 1  
  lecMulticastForwardVpi      = 0  
  lecMulticastForwardVci      = 33
```

lecConfigDirectInterface

La interfaz asociada con la VCC de configuración directa

lecConfigDirectVpi

VPI que identifica la VCC anterior si existe

lecConfigDirectVci

VCI que identifica la VCC anterior si existe

lecControlDirectInterface

La interfaz asociada con la VCC de control directo

lecControlDirectVpi

VPI que identifica la VCC anterior si existe

lecControlDirectVci

VCI que identifica la VCC anterior si existe

lecControlDistributeInterface

La interfaz asociada con la VCC de distribución de control

lecControlDistributeVpi

VPI que identifica la VCC anterior si existe

lecControlDistributeVci

VCI que identifica la VCC anterior si existe

lecMulticastSendInterface

La interfaz asociada con la VCC de envío de multidifusión

lecMulticastSendVpi

VPI que identifica la VCC anterior si existe

lecMulticastSendVci

VCI que identifica la VCC anterior si existe

lecMulticastForwardInterface

La interfaz asociada con la VCC de reenvío de multidifusión

lecMulticastForwardVpi

VPI que identifica la VCC anterior si existe

lecMulticastForwardVci

VCI que identifica la VCC anterior si existe

statistics

Visualiza la Tabla de estadísticas MIB del LEC.

Ejemplo:

```
LEC+ mib statistics
```

```
lecStatisticsTable:
  lecArpRequestsOut      = 1
  lecArpRequestsIn      = 0
  lecArpRepliesOut      = 0
  lecArpRepliesIn       = 1
  lecControlFramesOut   = 2
  lecControlFramesIn    = 2
  lecSvcFailures        = 1
```

lecArpRequestsOut

Número de peticiones ARP de LE enviadas por este LEC

lecArpRequestsIn

Número de peticiones ARP de LE recibidas por este LEC

lecArpRepliesOut

Número de respuestas ARP de LE enviadas por este LEC

lecArpRepliesIn

Número de respuestas ARP de LE recibidas por este LEC

lecControlFramesOut

Número de paquetes de control enviados por este LEC

lecControlFramesIn

Número de paquetes de control recibidos por este LEC

lecSvcFailures

El número total de:

Supervisión de LE Clients

- SVC de LAN Emulation de salida que este cliente ha intentado pero no ha podido abrir
- SVC de LAN Emulation de entrada que este cliente ha intentado pero no ha podido establecer
- SVC de LAN Emulation de entrada que este cliente ha rechazado por razones de seguridad o de protocolo

status Lista los estados MIB.

Ejemplo:

```
LEC+ mib status
lecStatusTable:
  lecPrimaryAtmAddress = 39.84.0F.00.00.00
  Client ATM address= = 00.00.00.00.00.01.10.00.5A.00.DE.AD.03
  lecId = 1 Assigned by LES
  lecInterfaceState = Operational State of the LEC
  lecLastFailureRespCode = None Error code from last
  lecLastFailureState = Initial State failed Config/Join resp.
  lecProtocol = 1 Protocol specified by
  lecVersion = 1 LEC in Join requests.
  lecTopologyChange = False LEC Protocol Version
  lecConfigServerAtmAddress = 00.00.00.00.00.00. of above
  lecConfigSource = Did not use LECS
  lecActualLanType = 802.3 - Ethernet Frame format currently
  lecActualMaxDataFrameSize = 1516 used by LEC
  lecActualLanName = ETH Name of emulated LAN
  lecActualLesAtmAddress = 39.84.0F.00.00.00. that LEC joined.
  lecProxyClient = False Is LES acting like a
  proxy ?
```

QoS Information

Utilice el mandato **qos-information** para obtener el indicador LEC x QoS+ desde el cual puede supervisar la Calidad de los servicios, tal como se describe en la sección Quality of Service Monitoring Commands de la publicación *Utilización y configuración de las características*.

Sintaxis:

qos-information

Trace

Utilice el mandato **trace** para activar o desactivar el rastreo de paquetes en el LEC. Consulte la sección “Mandatos de supervisión de rastreo de paquetes” en la página 201 para obtener más información.

Utilice el mandato **trace mac-address** para limitar los datos rastreados. Sólo se rastreará un paquete si se ha ejecutado lógicamente AND en su dirección MAC de destino o de origen con la máscara MAC de rastreo igual a la dirección MAC de rastreo en la que se ha ejecutado lógicamente AND con la máscara MAC de rastreo.

Sintaxis:

trace

Mandatos de supervisión LLC

Esta sección resume y explica todos los mandatos LLC. Estos mandatos, que aparecen en la Tabla 51, le permiten supervisar el LLC mientras pasa paquetes a través de una red SNA.

Tabla 51. Resumen de los mandatos de supervisión LLC

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página 10.
List	Visualiza información de configuración.
Set	Permite al usuario configurar dinámicamente los parámetros LLC que son válidos para la vida de la sesión.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página 11.

List

Utilice el mandato **list** para visualizar la información de configuración.

Sintaxis:

list

Set

Utilice el mandato **set** para configurar dinámicamente los parámetros LLC de una sesión LLC actual. Cualquier cambio que realice en los parámetros surtirá efecto para la vida de la sesión.

Atención: El cambio de los parámetros LLC desde los valores por omisión puede afectar a la forma en que funciona el protocolo LLC.

Sintaxis:

set *n2-max_retry cuenta*
n3-frames-rcvd-before-ack cuenta
nw-acks-to-inc-ww cuenta
t1-reply-timer segundos
t2-receive-ack-timer segundos
ti-inactivity-timer segundos
tw-transmit-window segundos

n2-max_retry

El número máximo de reintentos del protocolo LLC. Por ejemplo, N2 es el número máximo de veces que el LLC transmite un RR sin recibir un reconocimiento cuando caduca el temporizador de inactividad. El valor por omisión es 8. El mínimo es 1. El máximo es 127.

n3-frames-rcvd-before-ack

Este valor se utiliza con el temporizador T2 para reducir el tráfico de reconocimiento para las tramas I recibidas. Establezca este contador en un valor especificado. Cada vez que se recibe una trama I, se reduce este

Supervisión de LLC

valor. Cuando este contador llega a 0 o caduca el temporizador T2, se envía un reconocimiento. El valor por omisión es 1. El mínimo es 1. El máximo es 255.

nw-acks-to-inc-ww

Este campo se establece en el valor por omisión 1.

t1-reply-timer

Este temporizador caduca cuando LLC no puede recibir un reconocimiento o una respuesta necesarios de otra estación LLC. Cuando caduca este temporizador, se envía un RR con el bit de sondeo establecido y se vuelve a iniciar T1. Si el LLC no recibe ninguna respuesta después del número máximo de reintentos configurados (N2), el enlace subyacente se declara no operativo. El valor por omisión es 1. El mínimo es 1. El máximo es 256.

t2-receive-ack-timer

Este temporizador se utiliza para retrasar el envío de un reconocimiento para una trama recibida en formato I. Este temporizador se inicia cuando se recibe una trama I y se restablece cuando se envía un reconocimiento. Si este temporizador caduca, LLC2 envía un reconocimiento lo antes posible. Establezca este valor de modo que sea inferior al de T1. Esto asegura que el similar LLC2 remoto recibe el reconocimiento retrasado antes de que caduque el temporizador T1. El valor por omisión es 1 (100 ms). El mínimo es 1. El máximo es 2560.

Nota: Si este temporizador se establece en 1 (el valor por omisión) no se ejecutará (por ejemplo, **n3-frames-rcvd-before-ack=1**).

ti-inactivity-timer

Este temporizador caduca cuando LLC no recibe ninguna trama durante un período de tiempo especificado. Cuando este temporizador caduca, el LLC transmite un RR hasta que otro LLC responde o el temporizador N2 caduca. El valor por omisión es de 30 segundos. El mínimo es 1 segundo. El máximo es 256 segundos.

tw-transmit-window

Establece el número máximo de tramas I que pueden enviarse antes de recibir un RR. Suponiendo que el otro extremo de la sesión LLC pueda realmente recibir esta cantidad de tramas I consecutivas y que el dispositivo tenga suficiente memoria de almacenamiento dinámico para conservar estas copias hasta que se reciba un reconocimiento, si se incrementa este valor puede aumentarse la productividad. El valor por omisión es 2. El mínimo es 1. El máximo es 127.

Soporte para la reconfiguración dinámica de LEC

Esta sección describe la reconfiguración dinámica (DR) en la medida en que afecta a los mandatos Talk 6 y Talk 5.

Delete Interface de CONFIG (Talk 6)

LAN Emulation Client (LEC) soporta el mandato **delete interface** de CONFIG (Talk 6) sin ninguna restricción.

Activate Interface de GWCON (Talk 5)

LEC soporta el mandato **activate interface** de GWCON (Talk 5) sin ninguna restricción.

El mandato **activate interface** de GWCON (Talk 5) soporta todos los mandatos específicos de interfaz LEC.

Reset Interface de GWCON (Talk 5)

LEC soporta el mandato **reset interface** de GWCON (Talk 5) sin ninguna restricción.

El mandato **reset interface** de GWCON (Talk 5) soporta todos los mandatos específicos de interfaz LEC.

Mandatos de cambio temporal de GWCON (Talk 5)

LEC soporta todos los mandatos GWCON que cambian temporalmente el estado operativo del dispositivo. Estos cambios se pierden cuando se vuelve a cargar o se reinicia el dispositivo o cuando se ejecuta algún mandato reconfigurable dinámicamente.

Todas las modificaciones de LEC en Talk 5 efectúan a un cambio operativo inmediato.

Capítulo 28. Utilización de adaptadores de canal

Este capítulo describe cómo planificar la definición del sistema principal y el soporte de ESCON del 2216 y el Adaptador de canal paralelo (PCA). Incluye las secciones siguientes:

- La sección “Planificación de la definición de sistema principal”, proporciona información para ayudarle a planificar la definición de sistema principal.
- La sección “Planificación para el soporte de 2216” en la página 387, describe las consideraciones para el soporte del 2216 y de los adaptadores de canal en una red.
- La sección “Visión general del adaptador de canal” en la página 388, describe el soporte de adaptador de canal:
 - LCS (Estación de canal LAN) a través de la cual puede ejecutar TCP/IP
 - LSA (Link Services Architecture) a través de la cual puede ejecutar SNA jerárquica, incluyendo DLSw, APPN ISR o APPN HPR
 - MPC+ (Canal de diversas vías de acceso) a través del cual puede ejecutar APPN HPR, TCP/IP y HPDT UDP (UDP+)

Nota: UDP+ no está soportado en un Adaptador de Canal Paralelo (PCA).

- “Configuración de la interfaz de adaptador de canal” en la página 407
- “Mandatos de configuración de adaptador de canal” en la página 410

Planificación de la definición de sistema principal

Esta sección proporciona información para ayudarle a planificar la definición del sistema principal. Incluye información para la definición del sistema desde la perspectiva del sistema principal e información para la definición desde la perspectiva del 2216.

Antes de poder conectar el 2216 a un canal, debe configurarse correctamente el sistema principal. Los siguientes pasos son necesarios para definir la conexión del 2216 con el sistema principal. Estos pasos de definición debe realizarlos el programador del sistema.

1. Defina el 2216 en el subsistema de canal del sistema principal utilizando el Programa de configuración de la entrada/salida (IOCP) del sistema principal o el programa de Definición de configuración de hardware (HCD).
2. Defina el 2216 como una unidad de control en el sistema operativo del sistema principal.
3. Defina el 2216 y la configuración al programa del sistema principal (TCP/IP o VTAM).

Después de completar las definiciones del sistema principal, debe configurar las interfaces del canal 2216 utilizando la interfaz de línea de mandatos o utilizando el programa de configuración descrito en la publicación *Guía del usuario del Programa de Configuración para productos Nways Multiprotocol y Access Services*, GC10-3430. Muchos de los parámetros que proporcione al configurar el 2216 deben coincidir con los parámetros correspondientes de la definición del sistema principal.

Finalmente, será necesario configurar las estaciones para comunicarse a través del 2216 con las aplicaciones del sistema principal.

Las secciones siguientes describen la definición del sistema principal y proporcionan ejemplos de sentencias de configuración del sistema principal.

Definición de IOCP para el 2216

Las secciones siguientes describen ejemplos de definiciones IOCP para el 2216 con adaptadores de canal. La salida de las definiciones de dispositivo IOCP (Conjunto de datos de configuración de E/S o IOCDS) se puede generar utilizando MVS, VM, VSE o en un entorno autónomo. Consulte la publicación *IBM ES/9000 and ES/3090 Input/Output Configuration Program User's Guide Volume A04*, GC38-0097, para ver los detalles.

Ejemplo de definición IOCP para el canal ESCON

La Figura 19 muestra un ejemplo de una configuración ESCON. El sistema principal S/390 se divide en dos particiones lógicas (LP): LPA y LPB. Se configura una conexión en la vía de acceso 30 entre LPA y 2216A a través del conmutador 00 ESCD. LPA se conecta al puerto C0 ESCD y 2216A se conecta al puerto C1. La conexión entre el puerto C0 y C1 es dinámica.

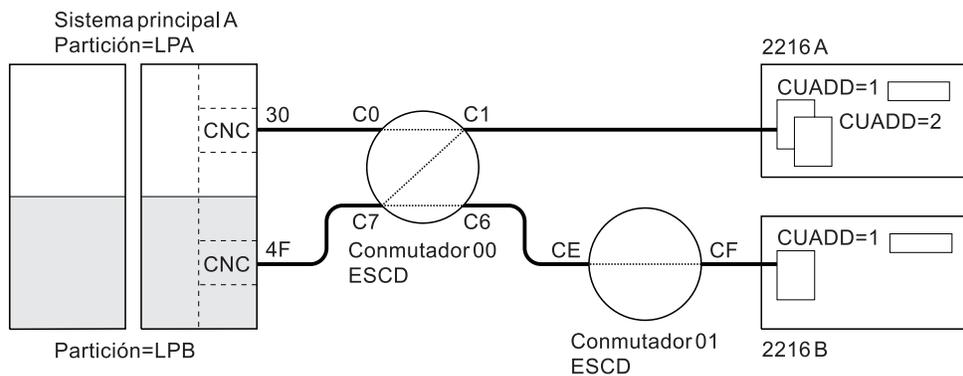


Figura 19. Ejemplo de configuración de canal ESCON

LPB de la vía de acceso 4F tiene una conexión con 2216A a través del conmutador ESCD 00 y una conexión con 2216B a través de los conmutadores ESCD 00 y 01. La conexión entre los puertos C7 y C6 es dinámica; la conexión entre los puertos ESCD CE y CF es dedicada.

Las definiciones de ejemplo siguientes coinciden con la Figura 19:

Definiciones de vías de canal:

```
CHPID    PATH=((30)),TYPE=CNC,PART=(LPA),SWITCH=00
CHPID    PATH=((4F)),TYPE=CNC,PART=(LPB),SWITCH=00
```

Definición de unidad de control y dispositivo para el 2216, con direccionamiento lógico = 1 para 2216A:

```
CNTLUNIT CUNUMBR=500,PATH=30,UNIT=3172,LINK=C1,      X
          UNITADD=(00,32),CUADD=1
IODEVICE ADDRESS=(500,32),CUNUMBR=500,UNIT=3172,    X
          UNITADD=00
```

Definición de unidad de control y dispositivo para el 2216 con direccionamiento lógico = 2 para 2216A:

```
CNTLUNIT CUNUMBR=600,PATH=4F,UNIT=3172,LINK=C1,      X
          UNITADD=(00,32),CUADD=2
IODEVICE ADDRESS=(600,32),CUNUMBR=600,UNIT=3172,    X
          UNITADD=00
```

Definición de unidad de control y dispositivo para el 2216, con direccionamiento lógico = 1 para 2216B:

CNTLUNIT	CUNUMBR=620,PATH=4F,UNIT=3172,LINK=C6, UNITADD=(20,32),CUADD=1	X
IODEVICE	ADDRESS=(620,32),CUNUMBR=620,UNIT=3172, UNITADD=20	X

Las macroinstrucciones IOCP del ejemplo:

- Asignan un CHPID a las particiones lógicas LPA y LPB.
- Definen la vía de canal 30 en el 2216 para la partición LPA y la vía de acceso de canal 4F para la partición LPB.
- Identifican el tipo de canal como un canal ESCON (CNC).
- Asignan los dos CHPID al conmutador ESCD número 00.
- Asocian las unidades de control número 500 y 600 a las direcciones lógicas 1 y 2 del 2216A y la unidad de control número 620 a la dirección lógica 1 del 2216B.
- Asignan la dirección de enlace C1 a las unidades de control 500 y 600 y la dirección de enlace C6 a la unidad de control 620.
- Definen las direcciones de unidad (subcanales) 00 a 1F a las unidades de control 500 y 600 y las direcciones de unidad 20 a 3F a la unidad de control 620.
- Identifican cada unidad de control como un dispositivo 3172.

Consideraciones:

1. El rango permitido de direcciones de dispositivo es de 00 a FF. El rango de direcciones del 2216 está limitado a 64 direcciones y sólo necesita que las direcciones definidas en el sistema principal se correlacionen con la dirección o direcciones configuradas en el 2216. El rango de direcciones se puede extender más allá de las direcciones que se utilizan actualmente, pero no pueden solapar las direcciones de otras unidades de control cableadas al mismo CHPID o canal.
2. La modalidad de operación de canal ESCON puede ser de tipo CNC para la modalidad de canal ESCON básica o CVC si hay un Conversor ESCON conectado.
3. El parámetro IODEVICE UNIT debe establecerse en 3172.
4. El número LINK especifica la dirección de enlace (número de puerto ESCD) al que está conectado el 2216. Cuando dos ESCD se conectan en serie, la dirección de enlace debe ser el número de puerto del ESCD que tiene la conexión dinámica y al que el 2216 está conectado.

Ejemplo de definición IOCP para el sistema principal EMIF

La Figura 20 en la página 370 muestra un ejemplo de una configuración ESCON que utiliza el Recurso de múltiples imágenes ESCON (EMIF). El sistema principal S/390 se divide en dos particiones lógicas (LP): LPA y LPB. Tanto LPA como LPB están conectados en la vía de acceso 30 al 2216 A a través del conmutador 00.

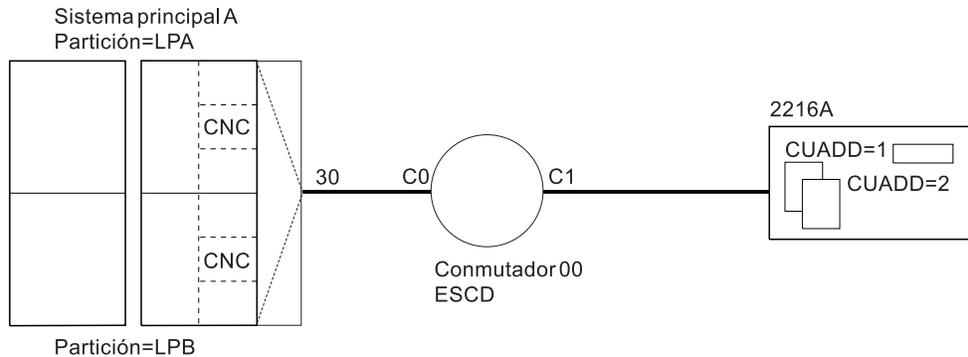


Figura 20. Ejemplo de configuración de sistema principal EMIF

Las definiciones de ejemplo siguientes coinciden con la Figura 20:

Definiciones de vía de acceso de canal:

CHPID PATH=((30)),TYPE=CNC,PART=(LPA,LPB),SWITCH=00

Definición de unidad de control y dispositivo para el 2216, con direccionamiento lógico = 1 para 2216A:

CNTLUNIT	CUNUMBR=500,PATH=30,UNIT=3172,LINK=C1,	X
	UNITADD=(00,32),CUADD=1	
IODEVICE	ADDRESS=(500,32),CUNUMBR=500,UNIT=3172,	X
	UNITADD=00	

Definición de unidad de control y dispositivo para el 2216, con direccionamiento lógico = 2 para 2216A:

CNTLUNIT	CUNUMBR=620,PATH=30,UNIT=3172,LINK=C1,	X
	UNITADD=(20,32),CUADD=2	
IODEVICE	ADDRESS=(620,32),CUNUMBR=620,UNIT=3172,	X
	UNITADD=20	

Las macroinstrucciones IOCP del ejemplo:

- Asignan un CHPID a las particiones lógicas LPA y LPB
- Definen la vía de acceso del canal 30 en el 2216 que se ha de compartir por la partición LPA y la partición LPB.
- Identifican el tipo de canal como un canal ESCON (CNC)
- Asignan el CHPID al conmutador ESCD número 00
- Asocian las unidades de control número 500 a la dirección lógica 1 y 620 a la dirección lógica 2 del 2216A
- Asignan la dirección de enlace C1 a las unidades de control 500 y 620
- Definen las direcciones de unidad (subcanales) 00 a 1F a la unidad de control 500 y de 20 a 3F a la unidad de control 620
- Identifican cada unidad de control como un dispositivo 3172.

Consideraciones:

1. El rango permitido de direcciones de dispositivo es de 00 a FF. El rango de direcciones del 2216 está limitado a 64 direcciones y sólo necesita que las direcciones definidas en el sistema principal se correlacionen con la dirección o direcciones configuradas en el 2216. El rango de direcciones puede extenderse más allá de las direcciones que se utilizan realmente para el 2216, pero no pueden solapar direcciones de otras unidades de control cableadas al mismo CHPID o canal.
2. La modalidad de operación de canal ESCON puede ser de tipo CNC para la modalidad de canal ESCON básica o CVC si hay un Conversor ESCON conectado.

3. El parámetro IODEVICE UNIT debe establecerse en 3172.
4. El número LINK especifica la dirección de enlace (número de puerto ESCD) al que está conectado el 2216. Cuando dos ESCD se conectan en serie, la dirección de enlace debe ser el número de puerto del ESCD que tiene la conexión dinámica y al que el 2216 está conectado.

Ejemplo de definición IOCP para el adaptador de canal paralelo (PCA)

La Figura 21 muestra un ejemplo de una configuración sencilla de Adaptador de canal paralelo en la que el tipo de canal se identifica como un canal multiplexor de bloques, TYPE=BL, en la vía de acceso 5.

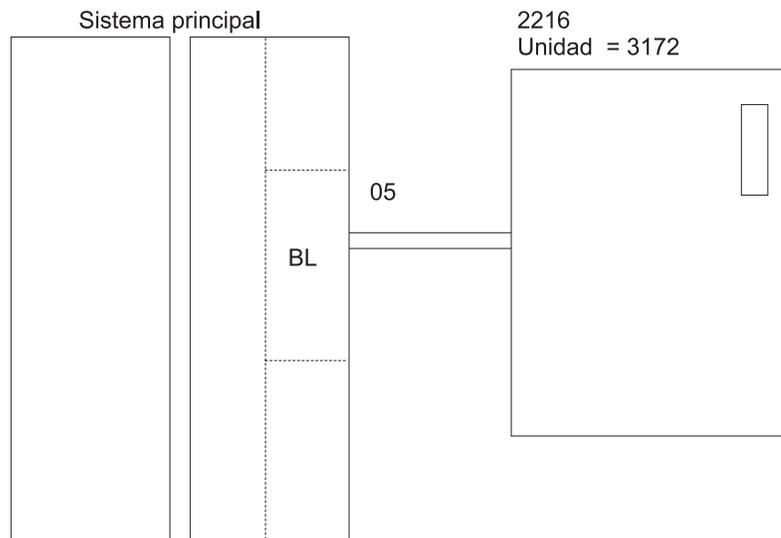


Figura 21. Ejemplo de configuración de adaptador de canal paralelo

La unidad de dispositivo de E/S del IBM 2216 aparece en el sistema principal como 3172 y debe definirse como 3172.

Las definiciones de ejemplo siguientes coinciden con la Figura 21:

```

CHPID      PATH=((05)),TYPE=BL
CNTLUNIT   CUNUMBR=640,PATH=05,                                X
           PROTOCL=S4,UNIT=3172,                                X
           SHARED=N,UNITADD=((40,32))
IODEVICE   UNIT=3172,ADDRESS=((640,32)),                          X
           STADET=N,CUNUMBER=640,TIMEOUT=Y

```

Las macroinstrucciones IOCP del ejemplo:

- Identifican el tipo de canal como un canal multiplexor de bloques (BL).
- Nombran la vía de acceso del canal 05 al que el PCA está conectado.
- Asignan la unidad de control número 640 al PCA.
- Especifican que el canal del sistema principal soporta hasta 4,5 MB de datos continuos (S4).
- Identifican la unidad de control como de tipo 2 donde se soportan simultáneamente múltiples peticiones de E/S (SHARED=N).
- Definen las direcciones de unidad 40 a 5F en el PCA (un rango de 32 direcciones).
- Identifican la unidad de control PCA como un dispositivo de tipo 3172.

Consideraciones:

1. El rango de direcciones para cada PCA debe ser pares contiguos de direcciones para TCP/IP, una sola dirección para VTAM y al menos un subcanal de lectura y un subcanal de grabación para MPC+.

El rango permitido de direcciones de dispositivo es de 00 a FF. Cada PCA de 2216 puede soportar un máximo de 32 subcanales. El PCA del 2216 no necesita un rango de 32 direcciones, sólo necesita que las direcciones definidas en el sistema principal se correlacionen con la dirección o direcciones configuradas para el PCA del 2216. Las direcciones utilizadas no pueden solapar las direcciones utilizadas por otras unidades de control o PCA cableados al mismo CHPID o canal.

2. El parámetro PROTOCL puede establecerse en los valores siguientes, dependiendo de las posibilidades del sistema principal:

- D** Modalidad Direct-Coupled Interlock (DCI)
- S** Velocidad máxima de corriente de datos de 3,0 MBps
- S4** Velocidad máxima de corriente de datos de 4,5 MBps

La modalidad de transferencia y la velocidad de transferencia del canal especificadas para el parámetro PROTOCL deben ajustarse al valor de PCA para la modalidad de transferencia y la velocidad de transferencia del canal.

3. El parámetro UNIT de las sentencias CNTLUNIT e IODEVICE debe establecerse en 3172.
4. Cuando el Conversor ESCON es la vía de acceso del canal, el parámetro CHPID TYPE debe establecerse en FX, de lo contrario se establece en BL.

Definición del 2216 en el sistema operativo

Las definiciones siguientes se aplican al 2216 con un adaptador de canal.

Definición del 2216 para VM/SP

El 2216 debe definirse en un sistema operativo VM/SP. Esta definición se consigue actualizando el archivo de configuración de E/S real (DMKRIO) con las entradas para el 2216 de las macros RDEVICE y RCTLUNIT. En el ejemplo siguiente, 640 es la dirección de la unidad base y el tamaño del rango de direcciones es 32.

```
RDEVICE ADDRESS=(640,32),DEVTYPE=3088
RCTLUNIT ADDRESS=640,CUTYPE=3088,FEATURE=32-DEVICE
```

Definición del 2216 para VM/XA y VM/ESA

El 2216 debe definirse en un sistema operativo VM/Extended Architecture (VM/XA o VM/ESA). Esta definición se consigue actualizando el archivo de configuración de E/S real (HCPRIO) con una entrada para el 2216 de la macro RDEVICE. En los ejemplos siguientes, 640 y 2A0 son las direcciones de la unidad de control base. El tamaño de rango de direcciones, tal como se define en UCW o IOCP, es 8 en ambos ejemplos.

El ejemplo siguiente es una definición VM/XA HCPRIO:

```
RDEVICE ADDRESS=(640,8),DEVTYPE=CTCA
```

El ejemplo siguiente es una definición VM/ESA HCPRIO:

```
RDEVICE ADDRESS=(2A0,8),DEVTYPE=CTCA
```

Definición del 2216 para MVS/XA y MVS/ESA sin HCD

Nota: Para definir un 2216 en un sistema MVS/ESA con HCD, consulte la sección "Definición del 2216 para MVS/ESA con HCD"

El 2216 debe definirse en un sistema operativo IBM Multiple Virtual Storage/Extended Architecture (MVS/XA) o MVS/ESA. Esta definición se consigue actualizando el Programa de control MVS con una entrada para el 2216 en la macro IODEVICE.

Para el caso de canales ESCON, un ejemplo de macro IODEVICE es:

```
IODEVICE UNIT=3172,ADDRESS(540,8)
```

Para canales paralelo, un ejemplo de macro IODEVICE es:

```
IODEVICE UNIT=CTC,ADDRESS(640,8)
```

Las direcciones de la unidad de control base son 640 y 540. El tamaño de rango de direcciones, tal como se define en UCW o IOCP, es 8 en ambos ejemplos.

Definición del 2216 para MVS/ESA con HCD

El componente de definición de configuración de hardware (HCD) de MVS/ESA SP Versión 4.2 y 4.3 con el APAR #OY67361 ofrece un método mejorado para definir la configuración de hardware del sistema para el 2216. Varios pasos complejos que son necesarios para entrar los datos de configuración de hardware se pueden realizar utilizando un diálogo interactivo con HCD.

Los datos de configuración necesarios para el 2216 son:

1. Cuando se utiliza HCD, con el APAR #OY67361, el 2216 se define como (UNIT=3172).

```
IODEVICE UNIT=3172,ADDRESS(740,8)
```

2. Sin HCD, el 2216 se define para:

- Canales paralelo como un dispositivo 3088 (UNIT = 3088 o CTC)

```
IODEVICE UNIT=CTC,ADDRESS(840,8)
```

- Canales ESCON como un dispositivo CTC serie (UNIT = SCTC)

```
IODEVICE UNIT=SCTC,ADDRESS(A40,8)
```

Notas:

1. Si está utilizando HCD para MVS Versión 4 para definir la conexión de sistema principal ESCON, necesitará el APAR #OY67361 para obtener el soporte UIM para la definición de dispositivo (UNIT=3172).
2. Cuando se migra la definición IOCP y las definiciones del sistema operativo al entorno HCD, es importante que todas las sentencias de dispositivo 2216 se cambien al tipo de dispositivo (UNIT=3172).

Definición del 2216 para VSE/ESA

El 2216 debe definirse en un sistema operativo VSE/ESA. Esta definición se consigue suministrando una sentencia ADD para cada dirección de unidad de canal en el momento de la carga del programa inicial (IPL). Codifique el tipo de dispositivo en la sentencia ADD como CTCA,EML tal como se muestra en el ejemplo siguiente:

```
ADD 640,CTCA,EML
```

La dirección de la unidad de control base es 640 en el ejemplo. Para los números de las direcciones de unidades de canal añadidas, aumente la macro de almacenamiento IOTAB con este número.

Definición del 2216 en programas del sistema principal

La sección contiene definiciones de configuración con ejemplos de definiciones del sistema principal necesarias para conectarse al adaptador de canal 2216.

Configuración del sistema principal para TCP/IP

TCP/IP puede conectarse al adaptador de canal 2216 utilizando LCS o MPC+. Cuando se utiliza MPC+, TCP/IP del sistema principal pasa a través de VTAM hasta el 2216.

Nota: Cuando se hace referencia a MPC+, el sistema principal utiliza el término HPDT MPC mientras que el 2216 utiliza el término MPC+.

TCP se configura en un sistema principal modificando el perfil de TCP/IP. El nombre por omisión para el conjunto de datos de perfil TCP/IP es TCPIP.PROFILE.TCPIP para MVS y PROFILE TCPIP para VM. Cada conexión de canal necesita:

- Una sentencia DEVICE para cada par o grupo de subcanales.
- Una sentencia LINK para cada interfaz LCS del 2216. Pueden definirse múltiples LINK para un solo DEVICE.
- Una sentencia LINK para cada dirección IP soportada a través de un Grupo MPC+. Sólo se puede definir un LINK para un solo DEVICE.
- Una entrada en la sentencia HOME para cada sentencia LINK.
- Entradas en la sentencia GATEWAY para el enlace que se ha de utilizar (si no se está utilizando ROUTED)
- Un mandato START para cada dispositivo

Consulte las publicaciones OS/390 TCP/IP OpenEdition para obtener más información sobre la configuración TCP/IP.

Configuración del sistema principal TCP/IP utilizando LCS: Estas son las sentencias necesarias para configurar TCP/IP en el sistema principal cuando se utiliza LCS:

Sentencias DEVICE y LINK: Los formatos de las sentencias DEVICE y LINK son:

```
DEVICE nombdispositivo subcanal LCS
LINK nombenlip tipoLAN númLAN nombdispositivo
```

donde:

nombdispositivo

es un nombre local para distinguir dispositivos. Necesita una sentencia START para este nombre de dispositivo al final del perfil, tal como se muestra en la sección “Ejemplo de mandatos TCP/IP cuando se utiliza LCS” en la página 376.

subcanal LCS

es el subcanal par de los dos subcanales LCS que utilizará esta conexión al 2216.

nombenlip

es el nombre local para distinguir los enlaces. Este nombre puede ayudarle a identificar el enlace que se está configurando.

tipoLAN

es el tipo de enlace.

númeroLAN

se obtiene del 2216 utilizando el mandato LIST NETS del submenú NETWORK adecuando.

Mandato HOME: Especifique las direcciones IP para cada conexión de canal utilizando el formato siguiente:

```
HOME direcipsistprinc nombenlip
```

donde:

direcipsistprinc

es la dirección IP del sistema principal para esta conexión con la red TCP/IP.

Nota: Esta dirección IP debe ser una dirección exclusiva de la misma subred IP que la dirección IP correspondiente codificada en el 2216.

nombenlip

es el nombre de enlace definido por la sentencia LINK, tal como se describe en la sección "Sentencias DEVICE y LINK" en la página 374.

Mandato GATEWAY: Especifique la información de direccionamiento si no está utilizando el servidor ROUTED.

```
GATEWAY red primer salto controlador tamaño paquete másc. subred valor subred
```

donde:

red es la dirección IP para la red. El valor por omisión es DEFAULTNET, que especifica una entrada de direccionamiento por omisión para cualquier red no direccionada explícitamente.

primer salto

Especifique uno de los siguientes:

Un signo igual (=) que significa que los mensajes se direccionan directamente a los destinos de esa red o directamente a ese sistema principal. No está soportado para DEFAULTNET.

La dirección Internet de una pasarela o direccionador al que puede llegar directamente y que reenvía los mensajes para la red o sistema principal de destino.

controlador

es el *nombenlip* definido por la sentencia LINK, tal como se describe en la sección "Sentencias DEVICE y LINK" en la página 374.

tamaño paquete

es la unidad máxima de transmisión en bytes para la red o el sistema principal.

másc. subred

es una máscara de bits que define los bits del campo del sistema principal que forman el campo de subred.

valor subred

es el valor del campo de subred.

Mandato START: Inicia todas las interfaces:

```
START nombdispositivo
```

donde:

nombdispositivo

es el parámetro definido por la sentencia DEVICE, tal como se describe en la sección “Sentencias DEVICE y LINK” en la página 374.

Ejemplo de mandatos TCP/IP cuando se utiliza LCS:

```
DEVICE LCS1 LCS 108
LINK TR1 IBMTR 0 LCS1
HOME
  16.51.136.199 TR1 1
GATEWAY
  16.51.136.201 = TR1 4000 HOST 2
  DEFAULTNET 16.51.136.201 TR1 4000 0
START LCS1
```

1 16.51.136.199 es la misma subred IP que la dirección IP de la interfaz LCS del 2216.

2 16.51.136.201 es la dirección IP de la interfaz LCS del 2216.

Configuración del sistema principal para TCP/IP utilizando MPC+: Estas son las sentencias necesarias para configurar TCP/IP en el sistema principal cuando se utiliza MPC+:

Sentencias DEVICE y LINK:

```
DEVICE nombdispositivo MPCPTP
LINK nombenlip MPCPTP nombdispositivo
```

donde:

nombdispositivo

es el nombre de la TRL que utilizará esta conexión con el 2216. Consulte la sección “Ejemplo de definición de 2216 en TCP/IP para MVS o VM para MPC+” en la página 379 para obtener información adicional.

MPCPTP

especifica un enlace de punto a punto MPC.

nombenlip

es un nombre de enlace para distinguir los enlaces. Este nombre puede ayudarle a identificar el enlace que se está configurando.

Mandato HOME: Especifique las direcciones IP para cada conexión de canal utilizando el formato siguiente:

```
HOME direcipsistprinc nombenlip
```

donde:

direcipsistprinc

es la dirección IP del sistema principal para esta conexión con la red TCP/IP.

Nota: Esta dirección IP debe ser una dirección exclusiva de la misma subred IP que la dirección IP correspondiente codificada en el 2216.

nombenlip

es el nombre de enlace definido por la sentencia LINK, tal como se describe en la sección “Sentencias DEVICE y LINK”.

Mandato GATEWAY: Especifique la información de direccionamiento si no está utilizando el servidor ROUTED.

```
GATEWAY red primer salto controlador tamaño paquete másc. subred valor subred
```

donde:

red es la dirección IP para la red. El valor por omisión es *redporomisión*, que especifica una entrada de direccionamiento por omisión para cualquier red no direccionada explícitamente.

primer salto

Especifique uno de los siguientes:

Un signo igual (=) que significa que los mensajes se direccionan directamente a los destinos de esa red o directamente a ese sistema principal. No está soportado para DEFAULTNET.

La dirección Internet de una pasarela o direccionador al que puede llegar directamente y que reenvía los mensajes para la red o sistema principal de destino.

controlador

es el *nombenlip* definido por la sentencia LINK, tal como se describe en la sección “Sentencias DEVICE y LINK” en la página 376.

tamaño paquete

es la unidad máxima de transmisión en bytes para la red o el sistema principal.

másc. subred

es una máscara de bits que define los bits del campo del sistema principal que forman el campo de subred.

valor subred

es el valor del campo de subred.

Mandato START: Inicia todas las interfaces:

```
START nombdispositivo
```

donde:

nombdispositivo

es el parámetro definido por la sentencia DEVICE, tal como se describe en la sección “Sentencias DEVICE y LINK” en la página 376.

Ejemplo de mandatos TCP/IP cuando se utiliza MPC+: Para MPC+:

```
DEVICE IPTRL1 MPCPTP
LINK LINK1 MPCPTP IPTRL1
HOME
    198.10.70.199 LINK1 1
GATEWAY
    198.10.70.203 = LINK1 16000 HOST 2
    DEFAULTNET 198.10.70.203 LINK1
START IPTRL1
```

1 198.10.70.199 es la misma subred IP que una de las direcciones IP de la interfaz MPC+ del 2216.

2 198.10.70.203 es una de las direcciones IP de la interfaz MPC+ del 2216.

Ejemplo de definición del 2216 en TCP/IP para MVS o VM para el LCS

El siguiente es un ejemplo de definiciones TCP/IP que se podrían proporcionar al sistema principal en el conjunto de datos del Perfil TCP/IP para configurar un dispositivo LCS. El nombre por omisión para el conjunto de datos de perfil TCP/IP es TCPIP.PROFILE.TCPIP para MVS y PROFILE TCPIP para VM.

Primero, se definen los dispositivos y enlaces del 2216 en TCP/IP.

Hay una sentencia DEVICE para cada par de subcanales que se utiliza para acceder a los 2216. La primera dirección especificada debe ser una dirección *par*. En este ejemplo, se definen dos dispositivos (pares de subcanales): uno en la dirección 640 y otro en la dirección 642. Estos dispositivos podrían estar en el mismo 2216 o en dos diferentes. Se utiliza un tipo de dispositivo de LCS (Estación de canal LAN) para definir estos dispositivos en TCP/IP.

Hay una sentencia LINK para cada adaptador LAN que se puede acceder desde estos dispositivos. En este ejemplo, se asigna un Adaptador Ethernet/802.3 al dispositivo utilizando los subcanales 640 y 641, se asignan dos adaptadores de Red en Anillo al dispositivo utilizando 642 y 643 y un adaptador FDDI utilizando 644 y 645. Estos dos adaptadores de Red en Anillo están en el mismo 2216 porque están asociados con el mismo dispositivo. El número de LINK para cada adaptador (0 y 1 en este ejemplo) lo asigna el 2216 cuando se añade un adaptador al perfil.

Nota: Son necesarias dos direcciones de subcanal para el envío y la recepción (por ejemplo, 640 y 641), pero sólo se define la primera dirección.

```

DEVICE LCS1 LCS 640
LINK ETH1 ETHERor802.3 0 LCS1
DEVICE LCS2 LCS 642
LINK TR1 IBMTR 0 LCS2
LINK TR2 IBMTR 1 LCS2
DEVICE LCS3 LCS 644
LINK FD1 FDDI 0 LCS3

```

Nota: En este ejemplo, 0 y 1 son números de LAN para estas conexiones.

Esta sección del ejemplo de perfil TCP/IP define las direcciones de internet del sistema principal locales:

```

HOME
193.5.2.1 ETH1
130.50.75.1 TR1
130.50.76.1 TR2
195.10.70.1 FD1

```

Esta sección del ejemplo de perfil TCP/IP representa la definición de pasarela LAN/WAN:

```

GATEWAY
Network First hop Driver Packet Size Subnet mask Subnet value
193.5.2 = ETH1 1500 0
130.50 = TR1 2000 0.0.255.0 0.0.75.0
130.50 = TR2 2000 0.0.255.0 0.0.76.0
195.10 = FD1 4000 0.0.255.0 0.0.70.0

```

Esta sección de ejemplo de perfil TCP/IP activa los dispositivos LCS:

```

START LCS1
START LCS2
START LCS3

```

Los ejemplos siguientes ilustran diversas maneras en que pueden especificarse los adaptadores LAN y enlazarse a pares de subcanal del perfil TCP/IP.

Se definen dos dispositivos LCS para los dos pares de subcanales 40,41 y 42,43 y cuatro adaptadores LAN en el 2216 de la manera siguiente:

```

DEVICE LCS1 LCS 640
LINK ETH1 ETHERNET 0 LCS1
LINK ETH2 ETHERNET 1 LCS1
DEVICE LCS2 LCS 642
LINK TRN1 IBMTR 0 LCS2
LINK TRN2 IBMTR 1 LCS2

```

Se definen cuatro dispositivos LCS para los cuatro pares de subcanales 40,41; 42,43; 44,45 y 46,47 y cuatro adaptadores LAN en el 2216 de la manera siguiente:

```
DEVICE LCS1 LCS 640
LINK ETH1 ETHERNET 0 LCS1
DEVICE LCS2 LCS 642
LINK ETH2 ETHERNET 1 LCS2
DEVICE LCS3 LCS 644
LINK TRN1 IBMTR 0 LCS3
DEVICE LCS4 LCS 646
LINK FD1 FDDI 0 LCS4
```

Se definen un dispositivo LCS para el par de subcanales 40,41 y cuatro adaptadores LAN en el 2216 de la manera siguiente:

```
DEVICE LCS1 LCS 640
LINK ETH1 ETHERNET 0 LCS1
LINK ETH2 ETHERNET 1 LCS1
LINK ETH3 ETHERNET 2 LCS1
LINK ETH4 ETHERNET 3 LCS1
```

Ejemplo de definición de 2216 en TCP/IP para MVS o VM para MPC+

El siguiente es un ejemplo de las definiciones TCP/IP que se proporcionarían al sistema principal en el conjunto de datos del Perfil TCP/IP para configurar un dispositivo MPC+. El nombre por omisión para el conjunto de datos de perfil TCP/IP es TCPIP.PROFILE.TCPIP para MVS y PROFILE TCPIP para VM.

Primero, en el sistema principal VTAM, defina una TRL en la que debe ejecutarse TCP/IP.

```
IPTRL VBUILD TYPE=TRL
IPTRL1 TRLE LNCTL=MPC,
      MAXBFRU=6,
      READ=(06),
      WRITE=(07)
REPLYTO=3.0
```

Notas:

1. Múltiples pilas TCP/IP pueden utilizar la misma TRL.
2. Consulte la sección “Configuración del sistema principal VTAM para MPC+ para IP” en la página 386 para ver más detalles.

Hay una sentencia DEVICE para cada TRL que TCP/IP ha de utilizar.

```
DEVICE IPTRL1 MPCPTP
```

Hay una sentencia LINK para cada dirección de internet de sistema principal local TCP/IP que utiliza la TRL. Para una pila TCP/IP determinada, sólo puede haber una sentencia LINK por TRL.

```
LINK LINK1 MPCPTP IPTRL1
```

Esta sección del ejemplo de perfil TCP/IP define las direcciones locales de internet de sistema principal y asocia las direcciones a un enlace:

```
HOME
198.10.70.199 LINK1 1
```

1 198.10.70.199 está en la misma subred IP que una de las direcciones IP de la interfaz MPC+ del 2216.

Esta sección del ejemplo de perfil TCP/IP representa la definición de la pasarela LAN/WAN:

GATEWAY

Network	First hop	Driver	Packet Size	Subnet	mask	Subnet value
198.10.70.203	=	LINK1	16000	HOST	1	
DEFAULTNET	198.10.70.203	LINK1	16000	0		

1 198.10.70.203 es una de las direcciones IP de la interfaz MPC+ del 2216.

Esta sección del ejemplo de perfil TCP/IP activa el dispositivo MPC+:

```
START IPTRL1
```

Nota: Antes de activar el dispositivo, active la TRL asociada si todavía no está activada.

Configuración del sistema principal para HPDT UDP:

¡Importante!

Antes de configurar el sistema principal S/390 para HPDT UDP, **debe** haber instalado el APAR #OW31305.

HPDT UDP sólo puede conectarse al 2216 a través de un Adaptador de canal ESCON que utilice MPC+.

Notas:

1. El 2216 hace referencia a HPDT UDP como UDP+.
2. UDP+ no está soportado en un Adaptador de canal paralelo (PCA).

HPDT UDP se configura y ejecuta utilizando OS/390 TCP/IP OpenEdition (OE) en el sistema principal. Por lo tanto, OS/390 TCP/IP OpenEdition debe estar instalado en el sistema principal.

Los mandatos HPDT UDP se utilizan para configurar y controlar los recursos HPDT UDP. Consulte la publicación *IBM OS/390 TCP/IP Update Guide* para ver los detalles sobre la instalación y utilización de OE para HPDT UDP.

Para configurar y activar una conexión HPDT UDP en el 2216, emita el mandato **oeifconfig**, mostrado en el ejemplo siguiente.

```
oeifconfig nombre_interfaz dirección_IP_origen dirección_IP_destino mtu nnnn
```

donde:

nombre_interfaz

es el nombre de la TRL para la conexión HPDT UDP.

Esto hará que se active la TRL si no está todavía activa.

Nota: Consulte la sección “Configuración del sistema principal VTAM para MPC+ para IP” en la página 386 para obtener información acerca de las TRL.

dirección_IP_origen

es la dirección IP local del sistema principal para la conexión HPDT UDP.

Esta dirección IP local debe estar en la misma subred IP que la dirección IP codificada para el manejador de red de UDP+ MPC+ en el 2216.

dirección_IP_destino

es la dirección IP de destino en el 2216 para esta conexión HPDT UDP.

Esta dirección IP de destino debe ser igual a la dirección IP codificada en el manejador de red UDP+ MPC+ en el 2216.

mtu nnnn

donde nnnn es el tamaño máximo de unidad de transmisión para la conexión HPDT UDP.

Este tamaño de mtu debe ser igual a los datos máximos codificados en el manejador de red UDP+ MPC+ del 2216. Si los valores no son iguales, la conexión HPDT UDP no se activará.

Nota: Puesto que se trata de una conexión de punto a punto, no hay ninguna necesidad de codificar el parámetro de máscara de red en este mandato.

Ejemplo de definición del 2216 en HPDT UDP para MVS o VM

Primero, en el sistema principal VTAM, defina una TRL en la que debe ejecutarse HPDT UDP.

```
UDPTRL VBUILD TYPE=TRL
TRL1   TRLE LNCTL=MPC,
        MAXBFRU=9,
        READ=(EA0),
        WRITE=(EA1),
        REPLYTO=3.0
```

Nota: Consulte la sección “Configuración del sistema principal VTAM para MPC+ para IP” en la página 386 para ver más detalles.

Después, vaya al entorno OE y emita el mandato siguiente:

```
oeifconfig trl1 198.10.60.199 198.10.60.203 mtu 16384
```

Bloques de control VTAM utilizados para configurar LSA en el sistema principal

La configuración del sistema principal VM o MVS necesita entradas en dos bloques de control VTAM:

- Archivo de definición de nodo principal del adaptador de comunicaciones externas (XCA)
- Archivo de configuración de nodo principal conmutado

Para obtener más información sobre la configuración de VTAM, consulte la publicación *IBM VTAM Resource Definition Reference*.

Archivo de definición de nodo principal XCA - ejemplo: La definición de un nodo principal XCA necesita la codificación de las sentencias de definición de VTAM para definir las características siguientes:

- Tipo de nodo (sentencia de definición VBUILD)
- Puerto utilizado por la LAN (sentencia de definición PORT)
- Líneas conmutadas conectadas a través de adaptador de canal 2216 (sentencias de definición GROUP, LINE y PU)

Debe codificar una sentencia de definición VBUILD y una sentencia de definición PORT para el nodo principal y las sentencias de definición GROUP, LINE y LU para los nodos secundarios.

También debe asignar los puntos de acceso a servicio (SAP) que se han de utilizar para cada canal virtual para una LAN o una LAN emulada.

Archivo de definición de nodo principal conmutado - ejemplo: El archivo de definición de nodo principal conmutado define las estaciones de trabajo a las que VTAM podrá acceder a través de adaptador de canal 2216 e identifica:

- El tipo de nodo (sentencia de definición VBUILD)
- Los recursos de red (sentencias de definición PU y LU)

Para definir la pasarela LAN/WAN del 2216 en VTAM, debe asociarse el adaptador LAN adecuado del IBM 2216 a una dirección de subcanal. Esta asociación se define en VTAM en una definición de nodo principal que está soportada por VTAM Versión 3 Release 4 y VTAM Versión 4 Release 1.

Configuración de la conexión LSA directa en el sistema principal VTAM

La configuración del sistema principal VM o MVS necesita entradas en dos bloques de control VTAM, el Archivo de definición del nodo principal XCA y el Archivo de definición de nodo principal conmutado. Consulte la sección “Bloques de control VTAM utilizados para configurar LSA en el sistema principal” en la página 381 para ver una descripción de la finalidad de estos bloques de control y las referencias a publicaciones VTAM.

Archivo de definición de nodo principal XCA - ejemplo:

```
ROUTE6B1 VBUILD TYPE=XCA
PORT6B1 PORT CUADDR=0CB,ADAPNO=0,TIMER=60,SAPADDR=08, C
                MEDIUM=RING
GRP6B1 GROUP DIAL=YES
*****
LN06B001 LINE ANSWER=ON,CALL=INOUT,ISTATUS=ACTIVE
PU06B001 PU ISTATUS=ACTIVE
```

Notas:

1. ADAPNO es el número de LAN para la interfaz LSA del 2216.
2. CUADDR es la dirección de canal. Esto se corresponde con la Dirección de dispositivo (tres caracteres hexadecimales que definen la dirección de canal) para la interfaz LSA del 2216.
3. MEDIUM=RING para Red en Anillo, MEDIUM=CSMACD para Ethernet y MEDIUM=FDDI para FDDI. Esto corresponde al valor especificado para LANtype para la interfaz 2216.

Archivo de definición de nodo principal conmutado - ejemplo:

```
PS06SW VBUILD TYPE=SWNET
PS06PU PU ADDR=01,IDBLK=05D,IDNUM=54445,MAXOUT=7,PACING=0,VPACING=0, C
                SSCPFM=USSSCS,MAXDATA=4105,MODETAB=LMT3270,MAXPATH=1, C
                ANS=CONT,ISTATUS=ACTIVE,DLOGMOD=B22NNE
PS06LU2 LU LOCADDR=02
PS06LU3 LU LOCADDR=03
PS06LU4 LU LOCADDR=04
PS06LU5 LU LOCADDR=05
```

Configuración de una conexión LSA APPN en el sistema principal VTAM

La configuración del sistema principal VM o MVS necesita entradas en dos bloques de control VTAM, el Archivo de definición del nodo principal XCA y el Archivo de definición de nodo principal conmutado. Consulte la sección “Bloques de control VTAM utilizados para configurar LSA en el sistema principal” en la página 381 para ver una descripción de la finalidad de estos bloques de control y las referencias a las publicaciones VTAM.

Archivo de definición de nodo principal XCA - ejemplo:

```

P15AP63X VBUILD TYPE=XCA
PORT63X PORT CUADDR=0CD,ADAPNO=0,TIMER=60,SAPADDR=04, C
MEDIUM=CSMACD
GRP63X GROUP DIAL=YES
*****
LN630403 LINE ANSWER=ON,CALL=INOUT,ISTATUS=ACTIVE
PU630403 PU ISTATUS=ACTIVE

```

Notas:

1. ADAPNO es el número de LAN para la interfaz LSA del 2216.
2. CUADDR es la dirección de canal. Esto corresponde a la Dirección de dispositivo (dos caracteres hexadecimales que definen el byte inferior de la dirección de canal) para la interfaz 2216.
3. MEDIUM=RING para Red en Anillo y MEDIUM=CSMACD para Ethernet. Esto corresponde al valor especificado para Tipo de LAN para la interfaz LSA del 2216.

Archivo de definición de nodo principal conmutado - ejemplo:

```

LS601 VBUILD TYPE=SWNET
CS601 PU ADDR=02,CPNAME=C210,MAXOUT=7,PACING=0,VPACING=0, C
CPCP=YES,MAXDATA=4105,MODETAB=LMT3270,MAXPATH=10, C
CONNTYPE=APPN,DYNLU=YES

```

Configuración de una conexión LSA DLSw en el sistema principal VTAM

La configuración del sistema principal VM o MVS necesita entradas en dos bloques de control VTAM, el Archivo de definición del nodo principal XCA y el Archivo de definición de nodo principal conmutado. Consulte la sección “Bloques de control VTAM utilizados para configurar LSA en el sistema principal” en la página 381 para ver una descripción de la finalidad de estos bloques de control y las referencias a las publicaciones VTAM.

Archivo de definición de nodo principal XCA - ejemplo:

```

P15AP60X VBUILD TYPE=XCA
PORT60X PORT CUADDR=0CC,ADAPNO=1,TIMER=60,SAPADDR=04, C
MEDIUM=CSMACD
GRP60X GROUP DIAL=YES
*****
LN600403 LINE ANSWER=ON,CALL=INOUT,ISTATUS=ACTIVE
PU600403 PU ISTATUS=ACTIVE
LN600404 LINE ANSWER=ON,CALL=INOUT,ISTATUS=ACTIVE
PU600404 PU ISTATUS=ACTIVE

```

Notas:

1. ADAPNO es el número de LAN para la interfaz LSA del 2216.
2. CUADDR es la dirección de canal. Esto corresponde a la Dirección de dispositivo (dos caracteres hexadecimales que definen el byte inferior de la dirección de canal) para la interfaz 2216.
3. MEDIUM=RING para Red en Anillo y MEDIUM=CSMACD para Ethernet. Esto corresponde al valor especificado para Tipo de LAN para la interfaz LSA del 2216.

Archivo de definición de nodo principal conmutado - ejemplo:

```

PSK5SW VBUILD TYPE=SWNET
PSK5PU PU ADDR=03,IDBLK=05D,IDNUM=07251,MAXOUT=7,PACING=0,VPACING=0, C
DLOGMOD=B22NNE, C
SSCPFM=USSSCS,MAXDATA=2000,MODETAB=LMT3270
PSK5LU2 LU LOCADDR=02
PSK5LU3 LU LOCADDR=03
PSK5LU4 LU LOCADDR=04
PSK5LU5 LU LOCADDR=05
PSK5LU6 LU LOCADDR=06

```

Configuración de una conversión local LSA DLSw en el sistema principal VTAM

La configuración del sistema principal VM o MVS necesita entradas en dos bloques de control VTAM, el Archivo de definición del nodo principal XCA y el Archivo de definición de nodo principal conmutado. Consulte la sección “Bloques de control VTAM utilizados para configurar LSA en el sistema principal” en la página 381 para ver una descripción de la finalidad de estos bloques de control y las referencias a las publicaciones VTAM.

Archivo de definición de nodo principal XCA - ejemplo:

```
P15AP60X VBUILD TYPE=XCA
PORT60X PORT CUADDR=0CC,ADAPNO=1,TIMER=60,SAPADDR=04, C
MEDIUM=CSMACD
GRP60X GROUP DIAL=YES
*****
LN600403 LINE ANSWER=ON,CALL=INOUT,ISTATUS=ACTIVE
PU600403 PU ISTATUS=ACTIVE
LN600404 LINE ANSWER=ON,CALL=INOUT,ISTATUS=ACTIVE
PU600404 PU ISTATUS=ACTIVE
```

Notas:

1. ADAPNO es el número de LAN para la interfaz LSA del 2216.
2. CUADDR es la dirección de canal. Esto corresponde a la Dirección de dispositivo (dos caracteres hexadecimales que definen el byte inferior de la dirección de canal) para la interfaz 2216.
3. MEDIUM=RING para Red en Anillo y MEDIUM=CSMACD para Ethernet. Esto corresponde al valor especificado para Tipo de LAN para la interfaz LSA del 2216.

Archivo de definición de nodo principal conmutado - ejemplo:

```
PS06SW VBUILD TYPE=SWNET,MAXDLUR=20
PS06PU PU ADDR=01,IDBLK=05D,IDNUM=54445,MAXOUT=7,PACING=0,VPACING=0, C
SSCPFM=USSSCS,MAXDATA=4105,MODETAB=LMT3270,MAXPATH=1, C
ANS=CONT,ISTATUS=ACTIVE,DLOGMOD=B22NNE
PS06LU2 LU LOCADDR=02
PS06LU3 LU LOCADDR=03
PS06LU4 LU LOCADDR=04
PS06LU5 LU LOCADDR=05
PSK5SW VBUILD TYPE=SWNET
PSK5PU PU ADDR=03,IDBLK=05D,IDNUM=07251,MAXOUT=7,PACING=0,VPACING=0, C
DLOGMOD=B22NNE, C
SSCPFM=USSSCS,MAXDATA=2000,MODETAB=LMT3270
PSK5LU2 LU LOCADDR=02
PSK5LU3 LU LOCADDR=03
PSK5LU4 LU LOCADDR=04
PSK5LU5 LU LOCADDR=05
PSK5LU6 LU LOCADDR=06
```

Los ejemplos siguientes muestran los macros XCA y SWNET que definen el nodo principal de la LAN para un adaptador de Red en Anillo y un adaptador Ethernet, respectivamente. En los ejemplos:

- GROUP1T, GROUP1E y GROUP1F representan los recursos conectados a la LAN que necesitan VBUILD TYPE=SWNET.
- GROUP2T, GROUP2E y GROUP2F representan una conexión para el nodo PU 5.

La tabla de modalidades y las entradas de modalidades por omisión sólo son ejemplos. Asegúrese de utilizar las tablas de modalidades y las entradas de modalidades definidas en la instalación.

```
TRLAN1 VBUILD TYPE=XCA
PORT1 PORT MEDIUM=RING,ADAPNO=0,CUADDR=644,TIMER=60,SAPADDR=4
GROUP1T GROUP DIAL=YES * Switched Attachment
LINE1TA LINE ANSWER=ON,CALL=INOUT,ISTATUS=ACTIVE
```

```

PU1TA  PU      ISTATUS=ACTIVE
LINE1TB LINE  ANSWER=ON, CALL=INOUT, ISTATUS=ACTIVE
PU1TB  PU      ISTATUS=ACTIVE
GROUP2T GROUP  DIAL=NO      * Leased Definition
LINE2T  LINE  USER=SNA    * Multi-domain Connection
PU2T    PU      MACADDR=400000000001, TGN=1, SUBAREA=2, SAPADDR=4, PUTYPE=5

ENLAN2  VBUILD TYPE=XCA
PORT2   PORT   MEDIUM=CSMACD, ADAPNO=0, CUADDR=645, TIMER=60, SAPADDR=4
GROUP1E GROUP  DIAL=YES    * Switched Attachment
LINE1EA LINE  ANSWER=ON, CALL=INOUT, ISTATUS=ACTIVE
PU1EA   PU      ISTATUS=ACTIVE
LINE1EB LINE  ANSWER=ON, CALL=INOUT, ISTATUS=ACTIVE
PU1EB   PU      ISTATUS=ACTIVE
GROUP2E GROUP  DIAL=NO    * Leased Definition
LINE2E  LINE  USER=SNA    * Multi-domain Connection
PU2E    PU      MACADDR=400000000002, TGN=2, SUBAREA=2, SAPADDR=4, PUTYPE=5

```

Los ejemplos siguientes son definiciones de nodos principales conmutados.

```

LS100SW VBUILD TYPE=SWNET, MAXGRP=400, MAXNO=400
CS100001 PU  ADDR=01, PUTYPE=2, MAXPATH=4, ANS=CONT, DLOGMOD=B22NNE,
          ISTATUS=ACTIVE, MAXDATA=521, IRETRY=YES, MAXOUT=7,
          PASSLIM=5, IDBLK=111, IDNUM=00001, MODETAB=LMT3270
          PATH DIALNO=0104400000000004, GRPNM=GROUP1T
S00102  LU  LOCADDR=2
CS100002 PU  ADDR=02, PUTYPE=2, MAXPATH=4, ANS=CONT, DLOGMOD=B22NNE,
          ISTATUS=ACTIVE, MAXDATA=521, IRETRY=YES, MAXOUT=7,
          PASSLIM=5, CPNAME=MYNS2, MODETAB=LMT3270
          PATH DIALNO=0104400000000005, GRPNM=GROUP1T
S00200  LU  LOCADDR=0, DLOGMOD=LU62MODE
S00202  LU  LOCADDR=2

CS100003 PU  ADDR=03, PUTYPE=2, MAXPATH=4, ANS=CONT, DLOGMOD=B22NNE,
          ISTATUS=ACTIVE, MAXDATA=521, IRETRY=YES, MAXOUT=7,
          PASSLIM=5, IDBLK=111, IDNUM=00003, MODETAB=LMT3270
          PATH DIALNO=0104400000000006, GRPNM=GROUP1E
S00302  LU  LOCADDR=2
CS100004 PU  ADDR=04, PUTYPE=2, MAXPATH=4, ANS=CONT, DLOGMOD=B22NNE,
          ISTATUS=ACTIVE, MAXDATA=521, IRETRY=YES, MAXOUT=7,
          PASSLIM=5, IDBLK=111, IDNUM=00004, MODETAB=LMT3270
          PATH DIALNO=0104400000000007, GRPNM=GROUP1E
S00402  LU  LOCADDR=2

CS100005 PU  ADDR=05, PUTYPE=2, MAXPATH=4, ANS=CONT, DLOGMOD=B22NNE,
          ISTATUS=ACTIVE, MAXDATA=521, IRETRY=YES, MAXOUT=7,
          PASSLIM=5, IDBLK=111, IDNUM=00005, MODETAB=LMT3270
          PATH DIALNO=0104400000000008, GRPNM=GROUP1F
S00502  LU  LOCADDR=2
CS100006 PU  ADDR=06, PUTYPE=2, MAXPATH=4, ANS=CONT, DLOGMOD=B22NNE,
          ISTATUS=ACTIVE, MAXDATA=521, IRETRY=YES, MAXOUT=7,
          PASSLIM=5, IDBLK=111, IDNUM=00006, MODETAB=LMT3270
          PATH DIALNO=0104400000000005, GRPNM=GROUP1F
S00602  LU  LOCADDR=2

```

Para obtener más información acerca de las definiciones de VTAM, consulte:

IBM VTAM V4R4 Network Implementation Guide, SC31-8370

IBM VTAM V4R4 Resource Definition Reference, SC31-8377

Configuración del sistema principal VTAM para MPC+ para APPN

La configuración del sistema principal VTAM para MPC+ para APPN necesita entradas en dos bloques de control VTAM, el Nodo principal SNA local y el Nodo principal de la Lista de recursos de transporte (TRL) y un cambio en los parámetros de arranque de VTAM. Una TRL corresponde a un grupo MPC+. Para obtener más información sobre la configuración de VTAM, consulte la publicación *IBM VTAM Resource Definition Reference*.

Nodo principal SNA local: Utilice las sentencias de definición siguientes para configurar un nodo principal SNA local en VTAM:

```

UTYLSNA VBUILD TYPE=LOCAL
UTYHCC1 PU      TRLE=UHCC1,XID=YES,CONNTYPE=APPN,CPCP=YES,HPR=YES

```

Nodo principal de la Lista de recursos de transporte (TRL):

```

BC4UTRL VBUILD TYPE=TRL
UHCC1   TRLE LNCTL=MPC,
        MAXBFRU=n,
        READ=(xxx1,xxx2,...),
        WRITE=(yyy1,yyy2,...),
        REPLYTO=3.0

```

C
C
C
C

donde:

n es el número de páginas de almacenamiento intermedio de 4 K que VTAM utiliza para recibir datos a través del canal.

xxx1,xxx2,...

son los números de subcanal de lectura. **1**

yyy1,yyy2,...

son los números de subcanal de grabación. **1**

1 No es necesario que los canales sean contiguos.

Los números de subcanal de lectura y grabación deben estar conectados a los configurados en el 2216 (por ejemplo, mediante un montaje del operador de mensajes o un mandato de conexión).

Nota: Un subcanal de “lectura” para VTAM es un subcanal de “grabación” para el 2216 y un subcanal de “grabación” para VTAM es un subcanal de “lectura” para el 2216.

Parámetros de arranque de VTAM: En el archivo de inicialización de VTAM ATCSTRxx, donde xx se define por el usuario, defina un nodo de red:

```

NODETYPE=NN

```

Puesto que se utiliza el direccionamiento de alto rendimiento (HPR), también debe añadir a este archivo:

```

HPR=YES

```

Nota: Sólo se soporta el HPR APPN en la interfaz MPC+. ISR APPN no está soportado.

Para activar la PU de APPN, active la TRLE asociada (si no está todavía activada) y, después, active la PU.

Consulte la publicación *IBM VTAM Operation* para obtener información acerca de los mandatos VTAM.

Configuración del sistema principal VTAM para MPC+ para IP

Nota: UDP+ no está soportado en un Adaptador de Canal Paralelo (PCA).

La configuración del sistema principal VTAM para MPC+ para TCP/IP o para HPDT UDP necesita una entrada en el bloque de control del Nodo principal de la Lista de recursos de transporte (TRL) de VTAM. Una TRL corresponde a un grupo MPC+. Para obtener más información sobre la configuración de VTAM, consulte la publicación *IBM VTAM Resource Definition Reference*.

Nodo principal de la Lista de recursos de transporte (TRL):

```
TRL      VBUILD TYPE=TRL
TRL1    TRLE LNCTL=MPC,
        MAXBFRU=n,
        READ=(xxx1,xxx2,...),
        WRITE=(yyy1,yyy2,...),
        REPLYTO=3.0
```

C
C
C
C

donde:

n es el número de páginas de almacenamiento intermedio de 4 K que VTAM utiliza para recibir datos a través del canal.

Nota: Para TCP/IP y HPDT UDP, MAXBFRU*4K debe ser mayor que los datos máximos codificados en el manejador de red MPC+ en el 2216.

Consulte las publicaciones *IBM OS/390 TCP/IP OpenEdition* y *IBM OS/390 Update Guide* para ver las restricciones adicionales relativas a MAXBFRU.

xxx1,xxx2,...

son los números de subcanal de lectura. **1**

yyy1,yyy2,...

son los números de subcanal de grabación. **1**

1 No es necesario que los canales sean contiguos.

Los números de subcanal de lectura y grabación deben coincidir con los configurados en el 2216 (por ejemplo, mediante un montaje del operador de mensajes o un mandato de conexión).

Nota: Un subcanal de “lectura” para VTAM es un subcanal de “grabación” para el 2216 y un subcanal de “grabación” para VTAM es un subcanal de “lectura” para el 2216.

Planificación para el soporte de 2216

Esta sección describe las consideraciones para dar soporte al 2216 y al adaptador de canal en una red. El análisis y la resolución de un problema de comunicaciones entre un adaptador de canal y un sistema principal o una LAN pueden necesitar que inicie los procedimientos para la resolución de problemas para el 2216.

El problema puede ser:

- Un problema de configuración o de definición del sistema principal
- Un problema de hardware o de software del 2216
- Un problema de canal entre el 2216 y el sistema principal
- Un problema de programa, recurso o hardware del sistema principal
- Un mal funcionamiento de un adaptador de la LAN, unidad de acceso u otro hardware
- Un problema de recurso o de programa de estación de trabajo de la LAN
- Un problema de comunicación entre el 2216 y la LAN
- Un problema al utilizar hardware o software

Las indicaciones de los problemas vienen en los informes del usuario o en los indicadores y códigos visualizados en el 2216 y en otros dispositivos o en los mensajes visualizados por programas. Estas indicaciones le ayudan a determinar si el problema es de hardware, de software o de usuario. También le ayudan a

Planificación para el soporte de 2216

determinar la ubicación (2216, LAN, sistema principal) y el componente (dispositivo, adaptador, canal o programa) de la red que tiene el problema.

La determinación de la naturaleza del problema indica a menudo los procedimientos, herramientas o información adicional que se pueden necesitar para la resolución. Las mismas herramientas, procedimientos e información también pueden indicar la necesidad de llamar al servicio técnico. Hay interfaces de resolución de problemas y de servicio (NetView, SNMP Client) disponibles para el cliente.

Análisis y resolución de problemas de adaptador de canal del 2216

Los procedimientos de determinación de problemas de adaptador de canal ESCON y PCA del 2216 que se describen en la publicación *2216 Nways Multiaccess Connector Service and Maintenance Manual, SY27-0350*, le ayudarán a corregir el problema, si es posible, y a determinar cuándo debe llamar al servicio técnico.

Reconfiguración

Es posible que cuando la red crezca, se reduzca o se reorganice deba reconfigurar los programas del sistema principal y los perfiles del 2216 para:

- Equilibrar el tráfico y la carga de trabajo de la red
- Migrar a nuevas versiones o releases de los programas del sistema principal
- Migrar a nuevas versiones o releases del 2216
- Cambiar los SYSGEN del sistema principal

Visión general del adaptador de canal

El Adaptador de canal ESCON y PCA proporciona al 2216 el acceso a aplicaciones de sistema principal SNA y TCP/IP desde las LAN, WAN y ATM.

La Figura 22 en la página 389 muestra un 2216 conectado a un sistema principal VTAM a través de un adaptador de canal. Cada adaptador de canal ESCON proporciona hasta 64 subcanales y hasta 32 manejadores de red virtuales asociados que pueden soportar los protocolos Estación de canal de LAN (LCS), Link Services Architecture (LSA) y Canal de diversas vías de acceso (MPC+). Cada Adaptador de canal paralelo (PCA) proporciona hasta 32 subcanales y 16 manejadores de red virtual asociados. Cada 2216 puede contener hasta cuatro adaptadores de canal.

Cada Adaptador de canal ESCON puede proporcionar conexiones para un máximo de:

- 32 sistemas principales o imágenes de sistemas principales lógicos utilizando LCS o MPC+ (cuando se utiliza con un Director ESCON)
- 64 sistemas principales o imágenes de sistemas principales lógicos utilizando LSA (cuando se utiliza con un Director ESCON)
- 15 imágenes de sistemas principales lógicos en procesadores con posibilidad de EMIF en modalidad de partición lógica cuando no hay ningún director ESCON presente.

Cada PCA puede proporcionar conexión con un sistema principal o una imagen de sistema principal lógico.

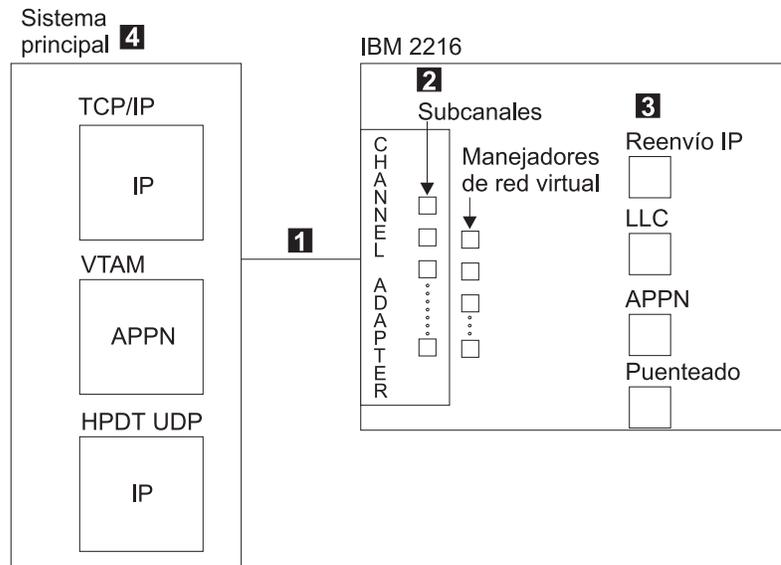


Figura 22. 2216 conectado a un sistema principal mediante un adaptador de canal ESCON/PCA - Vista lógica

- 1 A nivel físico, el Adaptador de canal ESCON proporciona una conexión de fibra óptica flexible con canales de comunicación del procesador del sistema principal. El nivel físico del PCA es considerablemente más complejo, necesita un par de cables de cobre muy grandes y un conjunto de uno a tres (dependiendo de la configuración) cables de cobre de par trenzado más pequeños para proporcionar la conexión final con el PCA.
- 2 A nivel lógico, el adaptador de canal proporciona hasta 64 *subcanales* y 32 *manejadores de red virtual* asociados.

Cada manejador de red virtual soporta uno de los protocolos siguientes:

- LCS** Estación de canal de LAN
- LSA** Link Services Architecture
- MPC+** Canal de diversas vías de acceso+

Para cada manejador de red virtual LCS, debe definir dos subcanales, uno para lectura y otro para grabación; puede definir hasta 32 manejadores de red virtual LCS para cada adaptador de canal ESCON y hasta 16 para cada PCA.

Para cada manejador de red virtual LSA, debe definir como mínimo un subcanal hasta un máximo de 64 subcanales. Puede definir hasta 32 manejadores de red virtual LSA para cada adaptador de canal ESCON y hasta 16 para cada PCA.

Para MPC+, puede definir hasta 64 subcanales. Debe tener como mínimo un subcanal de lectura y otro de grabación. Puede definir hasta 32 manejadores de red virtual MPC+ para cada adaptador de canal ESCON y hasta 16 para cada PCA.

Notas:

1. Puede configurar LCS y LSA en el mismo adaptador de canal.

Planificación para el soporte de 2216

2. Para la migración, puede configurar MPC+ en el mismo adaptador de canal que LCS/LSA. No está recomendado como solución a largo plazo. MPC+ combinado con otro tipo de interfaz virtual (LCS/LSA) en el mismo adaptador podría influir en la mejora del rendimiento proporcionada por la interfaz MPC+.
- 3** El adaptador de canal 2216 proporciona servicios para las funciones de Reenvío IP, Control de enlace lógico (LLC), Red avanzada de igual a igual (APPN) y de puente.
- 4** Los manejadores de red virtual proporcionan conexiones para transmitir y recibir paquetes de información para las aplicaciones del sistema principal, tal como se muestra en la Figura 23 y en la Figura 24 en la página 391.

Una vez instalado el adaptador de canal y configurado para LCS, LSA y MPC+, puede proporcionar:

- Una SNA jerárquica, incluyendo el tráfico DLSw y el tráfico APPN ISR y HPR que se ejecute en conexiones LSA. (DLSw y APPN necesitan un bucle de retorno LLC.)
- El tráfico TCP/IP que se ejecute en LCS y MPC+.
- El tráfico APPN HPR que se ejecute en MPC+.
- El tráfico HPDT UDP que se ejecute en MPC+.

Nota: UDP+ no está soportado en un Adaptador de Canal Paralelo (PCA).

La Figura 23 muestra el flujo básico para un adaptador de canal con LCS y LSA configurados y la Figura 24 en la página 391 muestra el flujo básico para un adaptador de canal para el que está configurado MPC+.

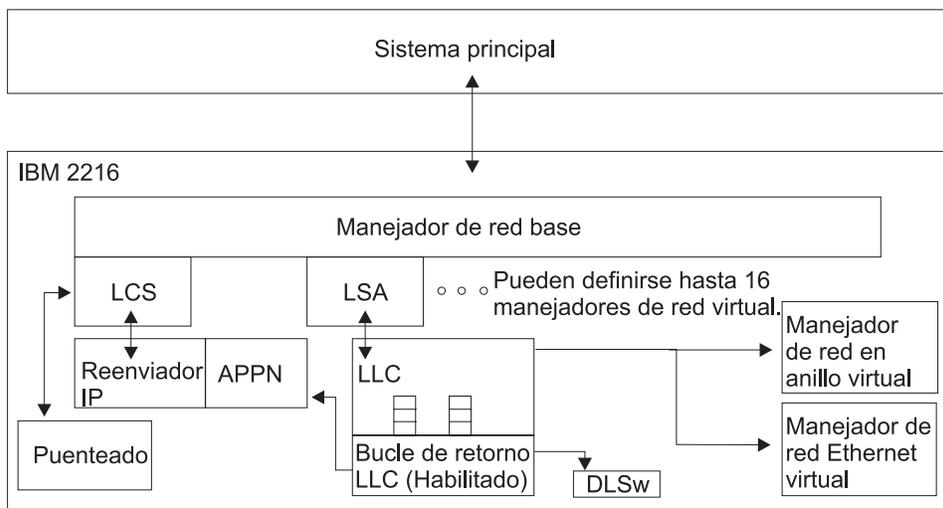


Figura 23. Manejadores de red virtual del 2216 para LCS y LSA

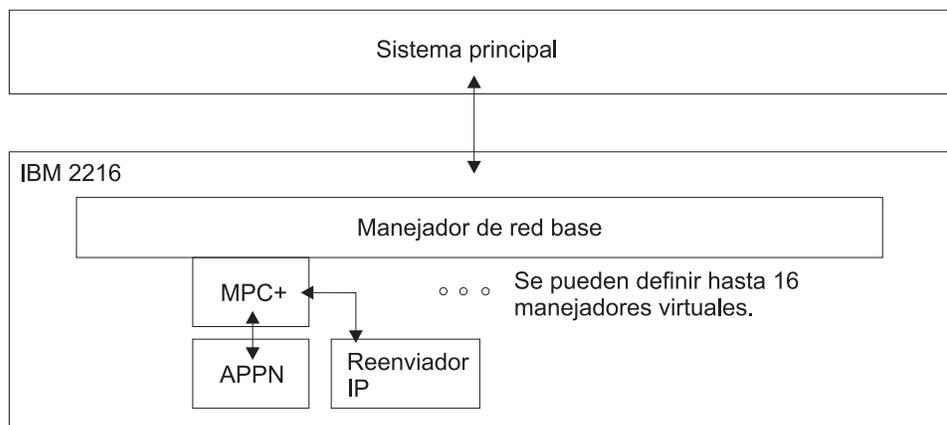


Figura 24. Manejadores de red virtual del 2216 para MPC+

Soporte de estación de canal LAN (LCS)

La Figura 25 muestra cómo fluyen los datos TCP/IP desde el sistema principal, a través de LCS y otros componentes de software 2216 para las LAN/WAN.

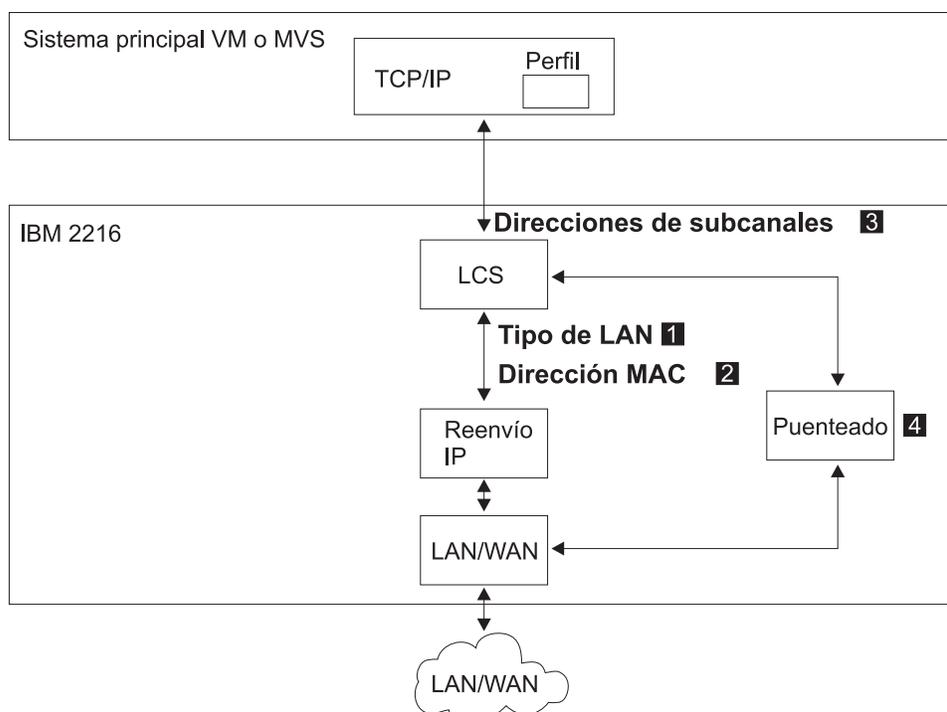


Figura 25. Configuración de los manejadores de red virtual de Estación de canal LAN (LCS). Esta figura muestra el flujo de LCS y resalta los parámetros clave del sistema principal y del 2216.

Configuración del 2216 para LCS

La Figura 25 muestra una conexión LCS. Para configurar el 2216 para LCS:

1. Configure el tipo de LAN (**1**), Ethernet, Red en Anillo o FDDI, para la conexión. Este es el tipo de trama que el sistema principal espera enviar y recibir.
2. Configure una dirección MAC exclusiva (**2**) para esta interfaz virtual.

Planificación para el soporte de 2216

Nota: Si el tipo de LAN es Ethernet, la dirección MAC debe estar en formato canónico.

- Configure el par de subcanales (**3**) utilizados por esta conexión, tal como se describe en la sección “Configuración de un subcanal LCS” en la página 412.
- (**4**) Si desea direccionar IP, configure una dirección IP y una máscara en el manejador de red virtual LCS. Consulte el capítulo Configuración IP de la publicación *Consulta de configuración y supervisión de protocolos Volumen 1* para obtener información sobre la configuración del direccionamiento IP. Si desea puentear IP, configure la función de puente en el manejador de red virtual LCS. La función de puente IP del manejador de red virtual LCS se llama *Paso a través TCP/IP*. Consulte la sección “Paso a través TCP/IP” para obtener más información sobre la configuración de la función de puente.

Debe configurar una dirección IP y una máscara. Consulte la publicación *Consulta de configuración y supervisión de protocolos Volumen 1*.

Hay parámetros opcionales:

maxdata

El tamaño máximo de los datos manejados por esta red virtual.

acklen

El tamaño (en bytes) de las tramas de reconocimiento en esta interfaz.

blktimer

El tiempo máximo (en milisegundos) que se ha de esperar antes de enviar un bloque de datos incompleto al sistema principal.

Para obtener información sobre las definiciones correspondientes del sistema principal, consulte la sección “Configuración del sistema principal para TCP/IP” en la página 374.

Paso a través TCP/IP

El Paso a través TCP/IP realiza una función de puente, en lugar de de direccionamiento, de las tramas IP recibidas en un manejador de red virtual LCS para una interfaz LAN o WAN. Para utilizar esta característica, debe configurar el puente en los manejadores de red virtual LCS y las interfaces LAN y WAN que desee interconectar. Consulte la sección Configuración y supervisión del puente de la publicación *Consulta de configuración y supervisión de protocolos Volumen 1*, para obtener más información sobre la configuración de la función de puente. El tipo de función de puente que configurará depende del tipo de LAN de las interfaces de red virtual LCS. La tabla siguiente muestra los parámetros de función de puente adecuados para cada tipo de LAN LCS.

Tipo LAN LCS	Tipo de función de puente	Tramas STE de reenvío
Red en Anillo	Direccionamiento de origen, transparente o ambos	Habilitado
Ethernet	Transparente	N/D
FDDI	Transparente	N/D

Nota: El protocolo de Árbol de expansión se inhabilita automáticamente en el manejador de red virtual LCS.

Atención: No puede configurar una dirección IP y una función de puente para una LCS. Si se especifican ambos, el programa de configuración funciona como si sólo hubiese especificado la opción de dirección IP. Si desea efectuar la función de puente de tramas IP, no especifique ninguna dirección IP.

Emulación 3172 utilizando el Paso a través LCS

El Paso a través LCS permite que el IBM 2216 funcione como un sustituto de 3172 en las redes TCP/IP. Las tramas recibidas de un sistema principal TCP/IP se pasan directamente a un adaptador LAN en sentido directo, pasando por alto el direccionador IP y las funciones de puente del IBM 2216. Las tramas IP y ARP recibidas por adaptador LAN asociado a la función de paso a través LCS se pasan directamente al manejador de red LCS para su entrega al sistema principal TCP/IP. El IBM 2216 sustituye la función LCS de 3172 sin necesidad de cambiar la topología de la red IP ni de añadir saltos de puentes adicionales.

El ejemplo siguiente describe la configuración de Paso a través LCS:

```
*t 6
Gateway user configuration
Config>add dev esc
Device Slot #(1-8) [1]?3
Adding ESCON Channel device in slot 3 port 1 as interface #4
Use "net 4" to configure ESCON Channel parameters
Config>net 4
ESCON Config>add lcs
ESCON Add Virtual>?
LANtype
MAC address
MAXdata
BLKtimer
ACKlen
SUBchannels
ENable 3172 Emulation
Exit
ESCON Add Virtual>enable
Enabling LCS 3172 Emulation for network 5.
Please set the Network link using the "NET" command.
ESCON Add Virtual>?
BLKtimer
ACKlen
SUBchannels
DISable 3172 Emulation
NET link
Exit
ESCON Add Virtual>net 0
ESCON Add Virtual>sub add
Please add or configure one subchannel for an LCS virtual interface.
Although LCS requires two subchannels, it is only necessary to specify
one subchannel. An adjacent subchannel will be chosen such that the two
subchannels will form a sequential pair with the write subchannel (device
address is even) before the read subchannel (device address is odd).
ESCON Config LCS Subchannel>?
LINK address (ESCD Port)
LPAR number
CU logical address
Device address
Exit
ESCON Config LCS Subchannel>link f7
ESCON Config LCS Subchannel>lpar 0
ESCON Config LCS Subchannel>cu 0
ESCON Config LCS Subchannel>dev 20
ESCON Config LCS Subchannel>ex
ESCON Add Virtual>ex
ESCON Config>list
Net: 5 Protocol: LCS LAN type: Token Ring LAN number: 0
      3172 Emulation is enabled.
      MAC address: Obtained from net 0
      Block Timer: 5 ms ACK length: 10 bytes
ESCON Config>list all
Net: 5 Protocol: LCS LAN type: Token Ring LAN number: 0
      3172 Emulation is enabled.
      MAC address: Obtained from net 0
      Block Timer: 5 ms ACK length: 10 bytes
      Read Subchannels:
```

Planificación para el soporte de 2216

```

Sub 0  Dev addr: 21  LPAR: 0  Link addr: F7  CU addr: 0
Write Subchannels:
Sub 1  Dev addr: 20  LPAR: 0  Link addr: F7  CU addr: 0
    
```

ESCON Config>

Soporte de Link Services Architecture (LSA)

Link Services Architecture (LSA) permite que el sistema principal VTAM se comunique con el adaptador de canal del 2216.

La Figura 26 muestra cuatro tipos de conexiones LSA. Su configuración se describe en:

- “Configuración de una conexión LSA directa en el 2216” en la página 395
- “Configuración de una conexión LSA APPN en el 2216” en la página 396
- “Configuración de una conexión LSA DLSw en el 2216” en la página 397
- “Configuración de una conversión local LSA DLSw en el 2216” en la página 399

Para obtener información sobre las definiciones correspondientes del sistema principal, consulte la sección “Bloques de control VTAM utilizados para configurar LSA en el sistema principal” en la página 381.

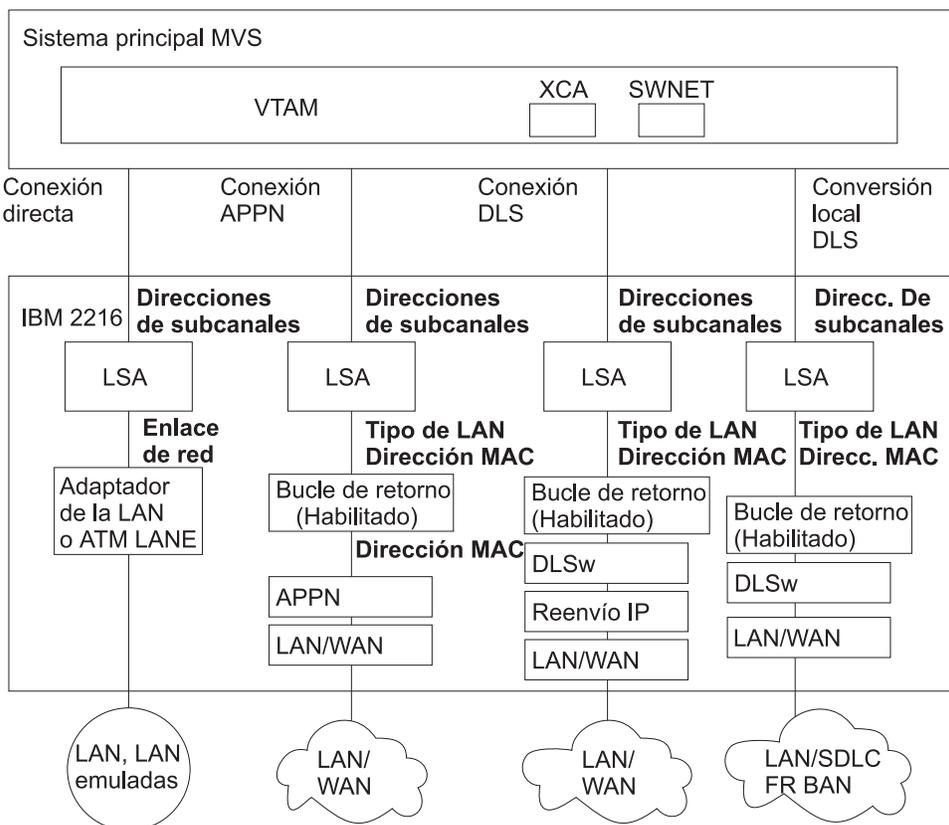


Figura 26. Configuración de manejadores de red virtual de Link Services Architecture (LSA)

Configuración de una conexión LSA directa en el 2216

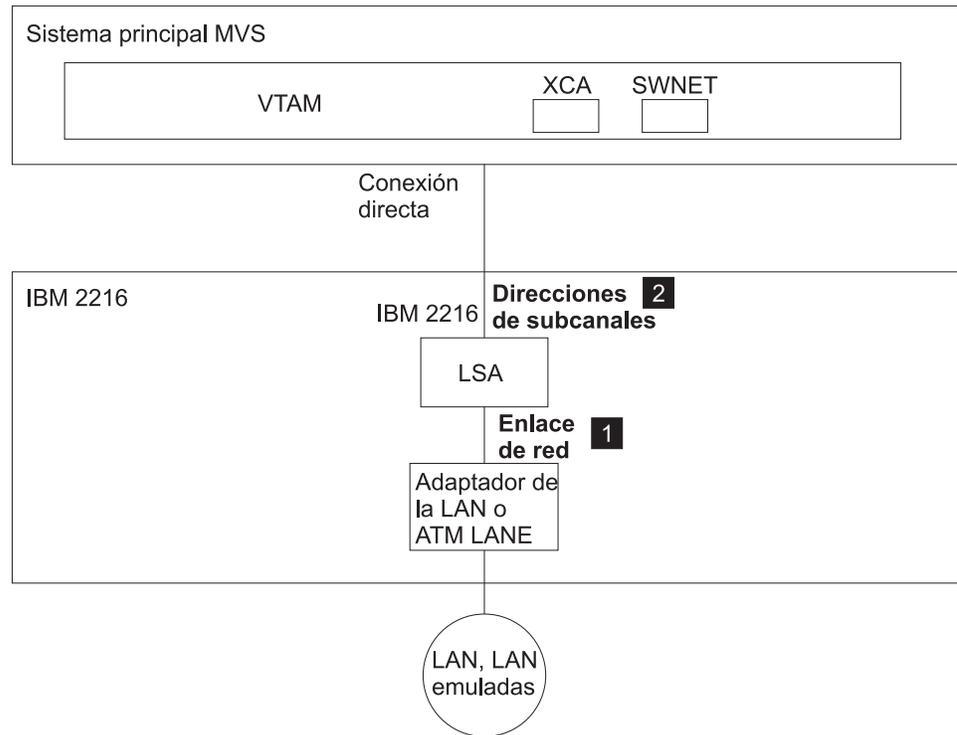


Figura 27. Configuración de manejadores de red virtual para la conexión LSA directa

La Figura 27 muestra una conexión LSA directa. Para configurar la conexión LSA:

1. Configure el enlace de red (**1**). Este es el número de interfaz de red del adaptador de la LAN al cual está enlazada la red LSA. Esta es la interfaz utilizada por el 2216 para transmitir los datos desde el sistema principal a la red.
2. Configure el subcanal o subcanales (**2**) utilizados por esta conexión, tal como se describe en la sección "Configuración de un subcanal LSA" en la página 416.

Hay parámetros opcionales:

maxdata

El tamaño máximo de los datos manejados por esta red virtual.

acklen

El tamaño (en bytes) de las tramas de reconocimiento en esta interfaz.

blktimer

El tiempo máximo (en milisegundos) que se ha de esperar antes de enviar un bloque de datos incompleto al sistema principal.

Nota: La red LSA leerá su dirección MAC en la interfaz de 2216 configurada con el mandato Net Link.

Para obtener información sobre las definiciones correspondientes del sistema principal, consulte la sección "Configuración de la conexión LSA directa en el sistema principal VTAM" en la página 382.

Planificación para el soporte de 2216

Configuración de una conexión LSA APPN en el 2216

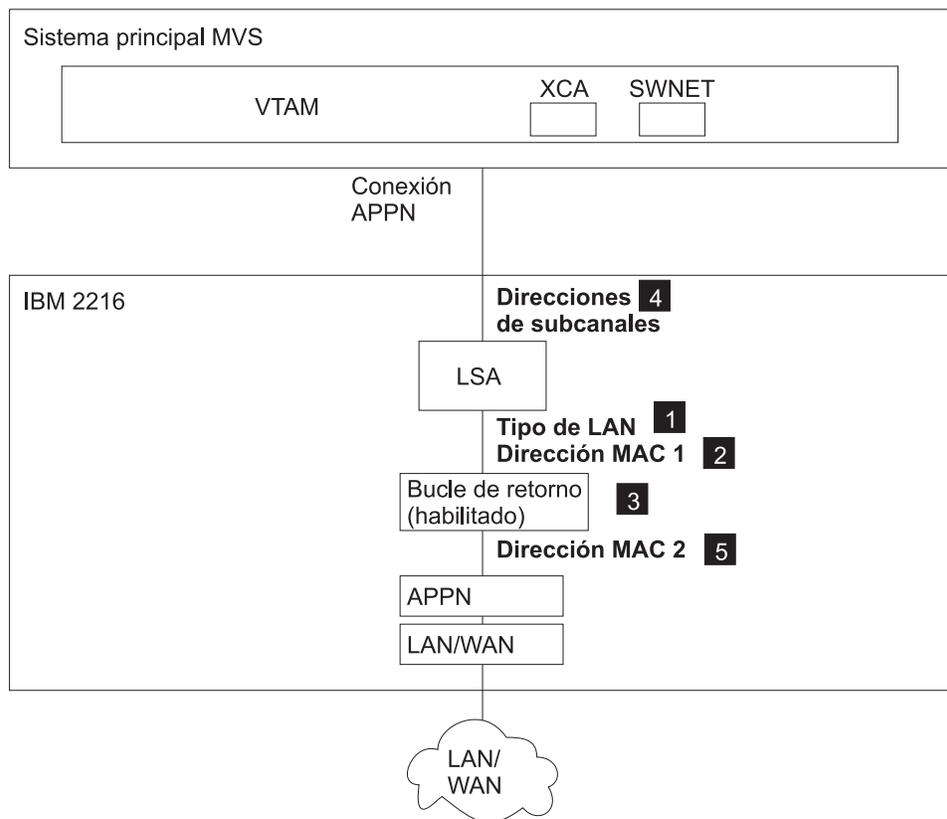


Figura 28. Configuración de manejadores de red virtual para la conexión LSA APPN

La Figura 28 muestra una conexión LSA APPN. Para configurar el 2216 para una conexión LSA APPN:

1. Habilite el bucle de retorno LSA (**3**) utilizando el mandato **enable**.
2. Configure el tipo de LAN (**1**), Ethernet o Red en Anillo

Nota: Debe configurar el mismo tipo de LAN para la red LSA y la red de bucle de retorno.

3. Configure una dirección MAC exclusiva (**2**) para identificar el extremo del sistema principal (VTAM) de la conexión de bucle de retorno.

Nota: Si el tipo de LAN es Ethernet, la dirección MAC debe estar en formato canónico.

4. Configure el subcanal o los subcanales (**4**) utilizados por esta conexión, tal como se describe en la sección “Configuración de un subcanal LSA” en la página 416.

Hay parámetros opcionales:

maxdata

El tamaño máximo de los datos manejados por esta red virtual.

acklen

El tamaño (en bytes) de las tramas de reconocimiento en esta interfaz.

blktimer

El tiempo máximo (en milisegundos) que se ha de esperar antes de enviar un bloque de datos incompleto al sistema principal.

5. Configure APPN para que utilice la red de bucle de retorno APPN. El puerto APPN debe estar configurado en la red de bucle de retorno APPN. Para configurar luego una estación de enlace APPN a través de este puerto APPN, la dirección MAC de destino de la definición de estación de enlace debe ser la de la red LSA.
6. Configure la dirección MAC 2 (**5**), una dirección MAC exclusiva para identificar el extremo del 2216 (APPN) de la conexión de bucle de retorno.

Nota: Si el tipo de LAN es Ethernet, la dirección MAC debe estar en formato canónico.

Para obtener información sobre las definiciones correspondientes del sistema principal, consulte la sección “Configuración de una conexión LSA APPN en el sistema principal VTAM” en la página 382.

Configuración de una conexión LSA DLSw en el 2216

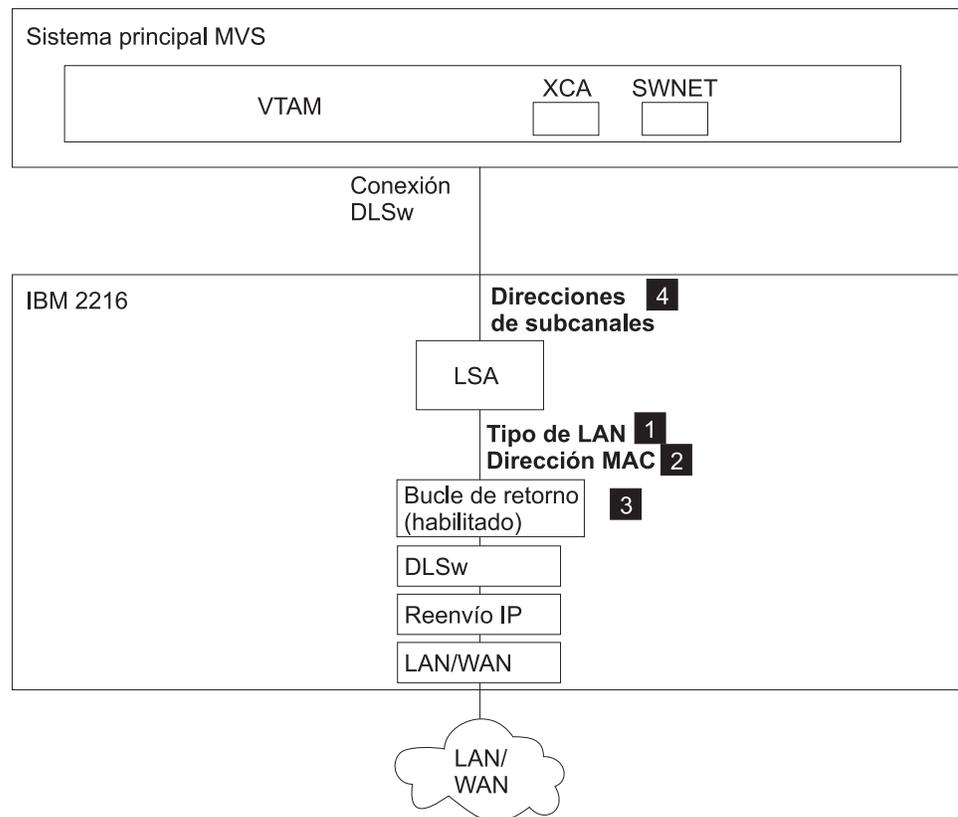


Figura 29. Configuración de manejadores de red virtual para la conexión LSA DLSw

La Figura 29 muestra una conexión LSA DLSw. Para configurar una conexión LSA DLSw:

1. Habilite el bucle de retorno LSA (**3**) utilizando el mandato **enable**.
2. Configure el tipo de LAN (**1**), Ethernet o Red en Anillo. Este es el tipo de trama que el sistema principal espera enviar y recibir.

Planificación para el soporte de 2216

3. Configure una dirección MAC exclusiva (**2**) para identificar el extremo del sistema principal (VTAM) de la conexión de bucle de retorno.

Nota: Si el tipo de LAN es Ethernet, la dirección MAC debe estar en formato canónico.

4. Configure el subcanal o los subcanales (**4**) utilizados por esta conexión, tal como se describe en la sección “Configuración de un subcanal LSA” en la página 416.
5. Configure DLSw. La configuración de DLSw implica la habilitación de DLSw, el establecimiento del número de segmento DLSw, la adición del asociado DLSw TCP remoto y la apertura de los puntos de acceso a servicios (SAP) asociados con la interfaz de bucle de retorno que se utilizará para DLSw. Configure DLSw desde el indicador `config>`.

Habilite DLSw, utilizando el mandato `enable dls`.

Establezca el número de segmento DLSw utilizando el mandato `set srb`. El número de segmento DLSw debe ser exclusivo.

Añada el asociado DLSw TCP remoto utilizando el mandato `add tcp`.

Abra los SAP que se utilizarán con la interfaz de bucle de retorno LSA utilizando el mandato `open`. El mandato `open` le solicitará un número de interfaz. Entre el número de interfaz asignado a la interfaz de bucle de retorno LSA que se ha definido para utilizar con LDSw.

Para ver una descripción de los parámetros de configuración de DLSw, consulte el capítulo titulado “Utilización y configuración de DLSw” de la publicación *Consulta de configuración y supervisión de protocolos Volumen 1*.

Hay parámetros opcionales:

maxdata

El tamaño máximo de los datos manejados por esta red virtual.

acklen

El tamaño (en bytes) de las tramas de reconocimiento en esta interfaz.

blktimer

El tiempo máximo (en milisegundos) que se ha de esperar antes de enviar un bloque de datos incompleto al sistema principal.

Para obtener información sobre las definiciones correspondientes del sistema principal, consulte la sección “Configuración de una conexión LSA DLSw en el sistema principal VTAM” en la página 383.

Configuración de una conversión local LSA DLSw en el 2216

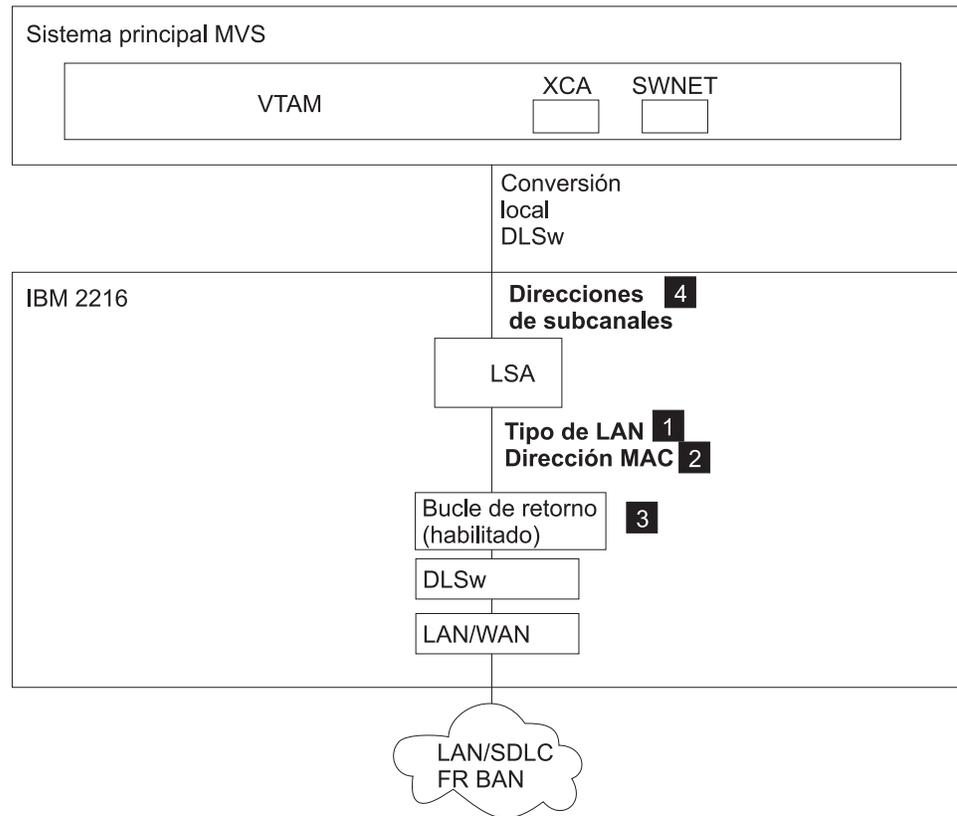


Figura 30. Configuración de manejadores de red virtual para la conversión local LSA DLSw

La Figura 30 muestra una configuración que soporta la conversión local LSA DLSw. Para configurar un 2216 para la conversión LSA DLSw:

1. Habilite el bucle de retorno LSA (**3**) utilizando el mandato **enable**.
2. Configure el tipo de LAN (**1**), Ethernet o Red en Anillo. Este es el tipo de trama que el sistema principal espera enviar y recibir.
3. Configure una dirección MAC exclusiva (**2**) para identificar el extremo del sistema principal (VTAM) de la conexión de bucle de retorno.

Nota: Si el tipo de LAN es Ethernet, la dirección MAC debe estar en formato canónico.

4. Configure el subcanal o los subcanales (**4**) utilizados por esta conexión, tal como se describe en la sección “Configuración de un subcanal LSA” en la página 416.
5. Configure DLSw. La configuración de DLSw implica la habilitación de DLSw, el establecimiento del número de segmento DLSw, la adición del asociado DLSw TCP local y la apertura de los puntos de acceso a servicios (SAP) asociados con la interfaz de bucle de retorno que se utilizará para DLSw. Configure DLSw desde el indicador `config>`.

Habilite DLSw, utilizando el mandato `enable dls`.

Establezca el número de segmento DLSw utilizando el mandato `set srb`. El número de segmento DLSw debe ser exclusivo. El número de segmento DLSw debe ser diferente de los números de segmentos asignados a otras interfaces.

Añada el asociado DLSw TCP local utilizando el mandato `add tcp`.

Planificación para el soporte de 2216

Abra los SAP que se utilizarán con la interfaz de bucle de retorno LSA utilizando el mandato open. El mandato open le solicitará un número de interfaz. Entre el número de interfaz asignado a la interfaz de bucle de retorno LSA que se ha definido para utilizar con DLSW.

Puede que sea necesario abrir los SAP y configurar la función de puente en las interfaces LAN/WAN locales. La apertura de los SAP y la configuración de la función de puente permite que se reenvíen las tramas de entrada a DLSw.

Nota: Cada interfaz LSA puede soportar hasta 10240 estaciones de enlace LLC por SAP. Una interfaz LSA puede soportar múltiples SAP.

Para ver una descripción de los parámetros de configuración de DLSw, consulte el capítulo titulado "Utilización y configuración de DLSw" de la publicación *Consulta de configuración y supervisión de protocolos Volumen 1*.

Hay parámetros opcionales:

maxdata

El tamaño máximo de los datos manejados por esta red virtual.

acklen

El tamaño (en bytes) de las tramas de reconocimiento en esta interfaz.

blktimer

El tiempo máximo (en milisegundos) que se ha de esperar antes de enviar un bloque de datos incompleto al sistema principal.

Soporte de canal de diversas vías de acceso+ (MPC+)

El canal de diversas vías de acceso+ (MPC+) permite que el sistema principal VTAM se comunique con el adaptador de canal del 2216. Un Grupo MPC+ es un conjunto de subcanales que contienen como mínimo un subcanal de lectura y otro de grabación, cuyos puntos finales convergen en una imagen de MPC+ común del sistema principal VTAM.

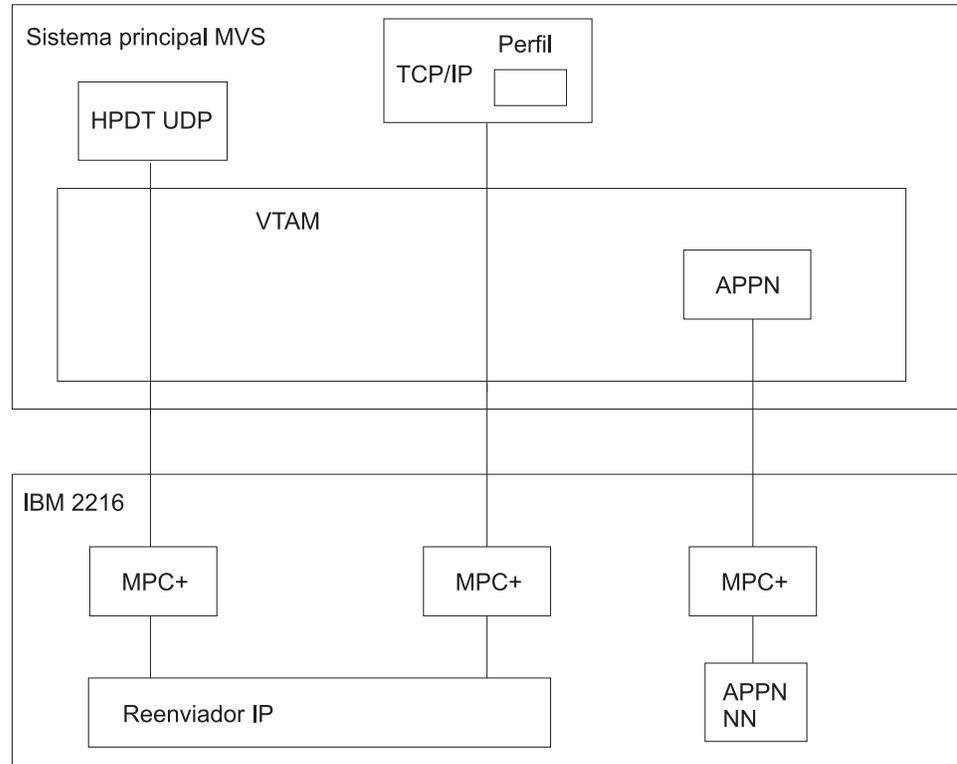


Figura 31. Diferentes tipos de conexiones MPC+.

Nota: UDP+ no está soportado en un Adaptador de Canal Paralelo (PCA).

La Figura 31 muestra los tres tipos de conexiones MPC+. Las secciones siguientes describen los tipos con más detalle:

- “Configuración del 2216 para APPN a través de MPC+” en la página 402
- “Configuración del 2216 para UDP+ a través de MPC+ (sólo para el adaptador de canal ESCON)” en la página 403
- “Configuración del 2216 para TCP/IP a través de MPC+” en la página 405

Para obtener información sobre las definiciones correspondientes del sistema principal, consulte la sección “Definición del 2216 en programas del sistema principal” en la página 374.

Para configurar un Grupo MPC+ en el 2216, configure una interfaz MPC+ en una interfaz base ESCON o PCA.

- Una conexión MPC+ con HPDT UDP del sistema principal necesita un Grupo MPC+ dedicado. Un Grupo MPC+ que está dedicado no puede compartirse por ningún otro usuario ni protocolo.

Nota: UDP+ no está soportado en un Adaptador de Canal Paralelo (PCA).

- Un Grupo MPC+ que no está dedicado puede compartirse por múltiples TCP/IP y por APPN.
- Puede haber múltiples Grupos MPC+ en un solo adaptador de canal.

Planificación para el soporte de 2216

Configuración del 2216 para APPN a través de MPC+

La Figura 32 muestra el flujo de MPC+ y resalta los parámetros clave en el sistema principal y en el 2216.

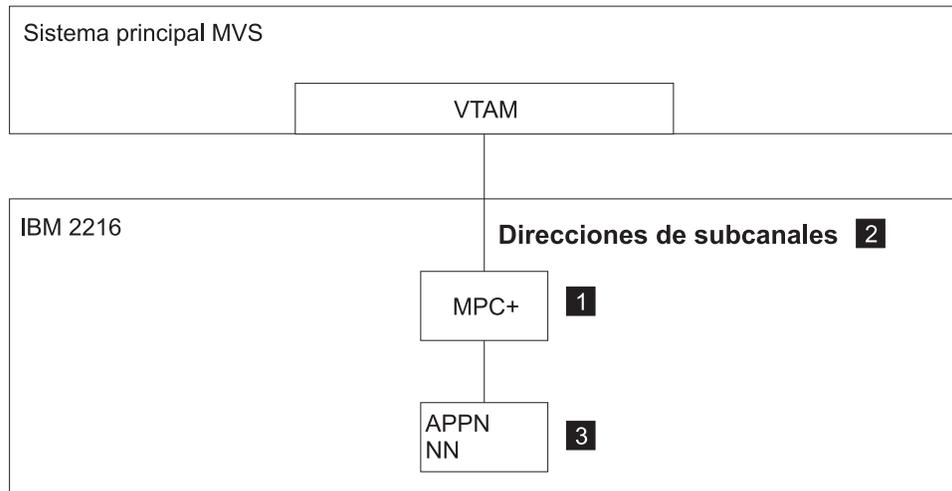


Figura 32. Configuración de manejadores de red virtual para APPN a través del Canal de diversas vías de acceso+ (MPC+)

La Figura 32 muestra los parámetros necesarios para configurar MPC+ para APPN.

1 Configure la interfaz virtual MPC+, tal como se describe en la sección “Configuración de una interfaz virtual MPC+” en la página 418.

2 Configure los subcanales para las conexiones de lectura y grabación con el sistema principal, tal como se describe en la sección “Configuración de un subcanal MPC+” en la página 420.

Nota: No habilite el uso exclusivo de UDP+ en la interfaz MPC+. Pase por alto el parámetro de inhabilitar bloqueo de datos de protocolo de salida. No se aplica y no surte ningún efecto para APPN.

Hay parámetros opcionales:

reply timeout

Temporizador para el tiempo de espera de XID2/Desconexión en milisegundos.

Es el período de tiempo que el Grupo MPC+ espera para escuchar a través del canal durante los intercambios XID2 y DISC antes de decidir que el otro extremo del canal no responde y que esta parte debe continuar con la activación o la desactivación del Grupo MPC+.

sequencing interval timer

Temporizador de secuencia de intervalos en milisegundos.

Este temporizador se utiliza para determinar si los datos orientados a la conexión fluyen sin problemas a través de la conexión en un Grupo MPC+. Los flujos de control MPC+ fluyen orientados a la conexión. Puesto que se ha de garantizar la entrega de estos mandatos a nivel de enlace, fluyen orientados a la conexión y se utiliza el Temporizador de secuencia de

Planificación para el soporte de 2216

intervalos para determinar si ha pasado el tiempo suficiente para que se haya producido la comprobación de la entrega del tráfico orientado a la conexión.

maxdata

Tamaño máximo de datos manejados por este manejador de red virtual.

acklen

El tamaño (en bytes) de las tramas de reconocimiento en esta interfaz.

blktimer

El tiempo máximo (en milisegundos) que se ha de esperar antes de enviar un bloque de datos incompleto al sistema principal.

3 Con las excepciones siguientes, APPN se configura a través de la interfaz MPC+ como se configura a través de otros tipos de interfaz:

- En el mandato “add port” de APPN, especifique el tipo de enlace MPC+.
- En el mandato “add port” de APPN, puede especificar el temporizador de secuencia de intervalos MPC+.

Para obtener información sobre las definiciones correspondientes del sistema principal, consulte la sección “Configuración del sistema principal VTAM para MPC+ para APPN” en la página 385.

Configuración del 2216 para UDP+ a través de MPC+ (sólo para el adaptador de canal ESCON)

La Figura 33 ilustra gráficamente una configuración UDP+ a través de MPC+.

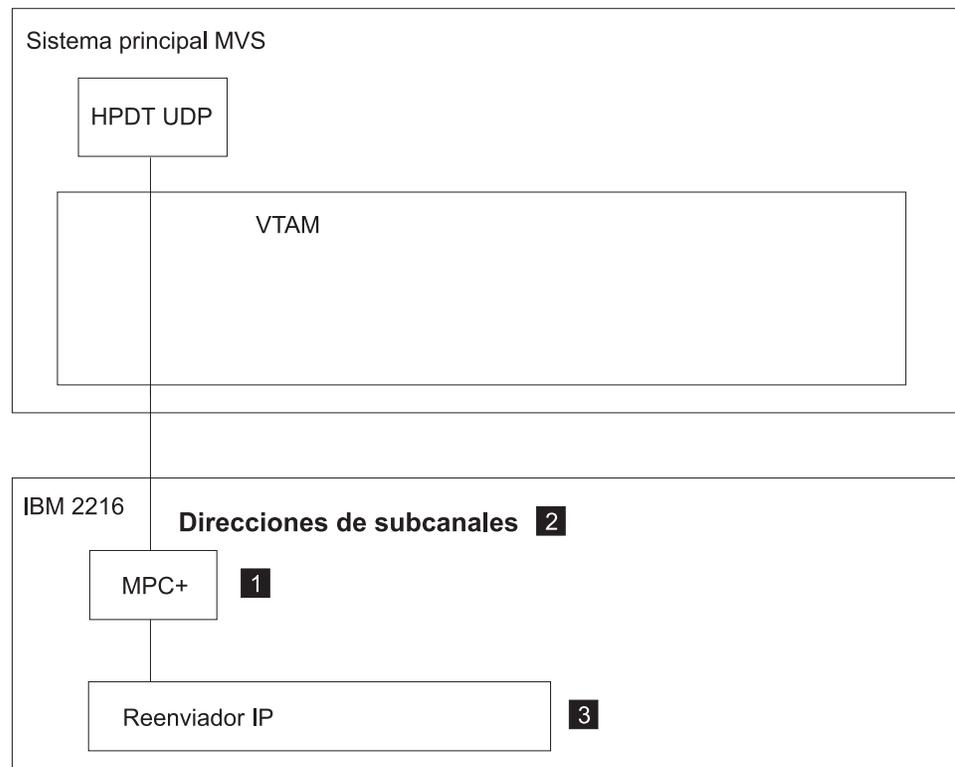


Figura 33. Configuración de manejadores de red virtual para UDP+ a través de MPC+

Planificación para el soporte de 2216

1 Configure la interfaz virtual MPC+, tal como se describe en la sección “Configuración de una interfaz virtual MPC+” en la página 418.

Habilite el uso exclusivo de UDP+ en la interfaz MPC+.

Hay parámetros opcionales:

reply timeout

Temporizador para el tiempo de espera de XID2/Desconexión en milisegundos.

Es el período de tiempo que el Grupo MPC+ espera para escuchar a través del canal durante los intercambios XID2 y DISC antes de decidir que el otro extremo del canal no responde y que esta parte debe continuar con la activación o la desactivación del Grupo MPC+.

sequencing interval timer

Temporizador de secuencia de intervalos en milisegundos.

Este temporizador se utiliza para determinar si los datos orientados a la conexión fluyen sin problemas a través de la conexión en un Grupo MPC+. Los flujos de control MPC+ están orientados a la conexión. Puesto que se ha de garantizar la entrega de estos mandatos a nivel de enlace, fluyen orientados a la conexión y se utiliza el Temporizador de secuencia de intervalos para determinar si ha pasado el tiempo suficiente para que se haya producido la comprobación de la entrega del tráfico orientado a la conexión.

maxdata

Tamaño máximo de datos manejados por este manejador de red virtual.

Nota: Este valor debe ser igual a la MTU codificada para HPDT UDP en el sistema principal.

acklen

El tamaño (en bytes) de las tramas de reconocimiento en esta interfaz.

blktimer

El tiempo máximo (en milisegundos) que se ha de esperar antes de enviar un bloque de datos incompleto al sistema principal.

outbound protocol blocking

Generalmente este parámetro debe dejarse habilitado. Consulte la sección “Configuración de una interfaz virtual MPC+” en la página 418 para ver los detalles.

2 Configure los subcanales para las conexiones de lectura y grabación con el sistema principal, tal como se describe en la sección “Configuración de un subcanal MPC+” en la página 420.

3 IP se configura a través de la interfaz MPC+ de la misma manera que se configura a través de otros tipos de interfaz; sin embargo:

- Sólo debe configurarse una dirección IP para una interfaz UDP+ MPC+. Esta dirección debe ser igual a la dirección_IP_destino codificada para HPDT UDP en el sistema principal.

Nota: Si se configuran más de una dirección IP, la última configurada es la que se utiliza.

Planificación para el soporte de 2216

- La dirección_IP_origen codificada para HPDT UDP en el sistema principal debe estar en la misma subred IP que la dirección IP configurada en el 2216 de la interfaz UDP+ MPC+.

Para obtener información sobre las definiciones correspondientes del sistema principal, consulte la sección “Configuración del sistema principal para HPDT UDP:” en la página 380.

Configuración del 2216 para TCP/IP a través de MPC+

La Figura 34 ilustra gráficamente una configuración TCP/IP a través de MPC+.

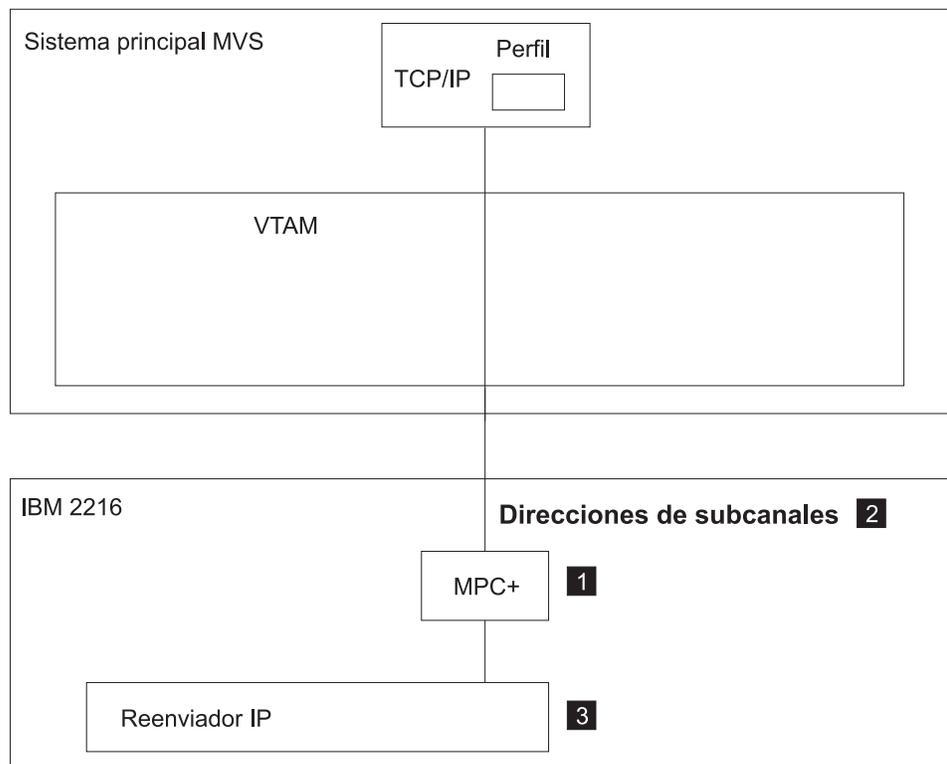


Figura 34. Configuración de manejadores de red virtual para TCP/IP a través de MPC+

1 Configure la interfaz virtual MPC+, tal como se describe en la sección “Configuración de una interfaz virtual MPC+” en la página 418.

Nota: No habilite el uso exclusivo de UDP+ en la interfaz MPC+. TCP/IP se configura en una interfaz MPC+ mediante la configuración de direcciones IP para el manejador de red MPC+ y no configurando la interfaz MPC+ para uso exclusivo de UDP+.

Hay parámetros opcionales:

reply timeout

Temporizador para el tiempo de espera de XID2/Desconexión en milisegundos.

Es el período de tiempo que el Grupo MPC+ espera para escuchar a través del canal durante los intercambios XID2 y DISC antes de decidir que el otro extremo del canal no responde y que esta parte debe continuar con la activación o la desactivación del Grupo MPC+.

Planificación para el soporte de 2216

sequencing interval timer

Temporizador de secuencia de intervalos en milisegundos.

Este temporizador se utiliza para determinar si los datos orientados a la conexión fluyen sin problemas a través de la conexión en un Grupo MPC+. Los flujos de control MPC+ fluyen orientados a la conexión. Puesto que se ha de garantizar la entrega de estos mandatos a nivel de enlace, fluyen orientados a la conexión y se utiliza el Temporizador de secuencia de intervalos para determinar si ha pasado el tiempo suficiente para que se haya producido la comprobación de la entrega del tráfico orientado a la conexión.

maxdata

Tamaño máximo de datos manejados por este manejador de red virtual.

Notas:

1. Este valor debe ser inferior o igual a la cantidad máxima de datos que el sistema principal puede manejar en la recepción a través del canal (es decir, MAXBFRU*4K, donde MAXBFRU es la TRLE VTAM correspondiente a esta interfaz MPC+ del 2216).
2. El 2216 no enviará nunca un paquete IP más largo que maxdata a través del Grupo MPC+. Sin embargo, dependiendo de los valores de maxdata configurados para otros manejadores de red virtual que utilizan la misma interfaz de canal base que esta interfaz MPC+, realmente el 2216 puede aceptar un paquete IP mayor del sistema principal.

acklen

El tamaño (en bytes) de las tramas de reconocimiento en esta interfaz.

blktimer

El tiempo máximo (en milisegundos) que se ha de esperar antes de enviar un bloque de datos incompleto al sistema principal.

outbound protocol blocking

Generalmente este parámetro debe dejarse habilitado. Consulte la sección “Configuración de una interfaz virtual MPC+” en la página 418 para ver los detalles.

2 Configure los subcanales para las conexiones de lectura y grabación con el sistema principal, tal como se describe en la sección “Configuración de un subcanal MPC+” en la página 420.

3 IP se configura a través de la interfaz MPC+ de la misma manera que se configura a través de otros tipos de interfaz; sin embargo:

- Se pueden establecer múltiples conexiones TCP/IP a través de interfaz MPC+ a través de una sola interfaz MPC+.
- Para establecer una conexión TCP/IP a través de MPC+, la dirección IP HOME de TCP/IP debe estar en la misma subred IP que una de las direcciones IP configuradas en la interfaz MPC+ del 2216.
- Si hay múltiples instancias de TCP/IP del sistema principal en la misma subred IP que la configurada para la interfaz MPC+ del 2216, se configurarán múltiples conexiones TCP/IP a través de MPC+ utilizando la misma dirección IP del 2216.

Para obtener información sobre las definiciones correspondientes del sistema principal, consulte la sección “Configuración del sistema principal para TCP/IP” en la página 374.

Configuración de la interfaz de adaptador de canal

Son necesarios los pasos siguientes para configurar la interfaz ESCON o PCA:

1. Acceda a la interfaz ESCON o PCA, tal como se describe en la sección “Acceso a la interfaz de canal” en la página 409. Esto hará que se defina la interfaz base.
2. Configure los manejadores de red virtual, tal como se describe en:
 - “Configuración de una interfaz virtual LCS” en la página 411
 - “Configuración de una interfaz virtual LSA” en la página 414
 - “Configuración de una interfaz virtual MPC+” en la página 418
3. Configure los subcanales:
 - “Configuración de un subcanal LCS” en la página 412
 - “Configuración de un subcanal LSA” en la página 416
 - “Configuración de un subcanal MPC+” en la página 420

Una vez se haya completado la configuración de ESCON o PCA del 2216,

- Configure los protocolos.
- Guarde la configuración.
- Rearranque el 2216 para activar los cambios.

Planificación para el soporte de 2216

Capítulo 29. Configuración y supervisión de los adaptadores de canal ESCON y paralelo

Este capítulo describe los mandatos de configuración y operativos de Enterprise Systems Connection (ESCON) y del Adaptador de canal paralelo. Contiene las secciones siguientes:

- “Acceso a la interfaz de canal”
- “Mandatos de configuración de adaptador de canal” en la página 410
- “Acceso al proceso de supervisión de interfaces de canal” en la página 431
- “Mandatos de supervisión de interfaces de canal” en la página 431
- “Mandatos de supervisión de interfaces LCS de adaptador de canal” en la página 436
- “Mandatos de supervisión de interfaces LSA de adaptador de canal” en la página 438
- “Mandatos de supervisión de interfaces MPC+ de adaptador de canal” en la página 441
- “Capítulo 30. Soporte para la reconfiguración dinámica del canal ESCON” en la página 447
- “Capítulo 31. Soporte para la reconfiguración dinámica del canal PCA” en la página 449
- “Capítulo 32. Soporte para la reconfiguración dinámica del canal virtual LSA” en la página 451
- “Capítulo 33. Soporte para la reconfiguración dinámica del canal virtual LCS” en la página 453
- “Capítulo 34. Soporte para la reconfiguración dinámica del canal virtual MPC” en la página 455
- “Capítulo 35. Soporte para la reconfiguración dinámica de la interfaz de bucle de retorno APPN” en la página 457

Para ver información adicional sobre la supervisión, consulte la publicación *Guía del usuario de software*.

Nota acerca de los ejemplos

Las secciones siguientes contienen ejemplos de configuraciones de interfaces ESCON y PCA. En las áreas en las que existe una diferencia significativa entre ESCON y PCA, se presentarán varios ejemplos.

Acceso a la interfaz de canal

Para acceder a la interfaz de adaptador de canal:

1. En el indicador OPCODE, entre **talk 6**. Por ejemplo:

```
* talk 6
  Config>
```

Después de entrar el mandato **talk 6**, se visualiza el indicador CONFIG (Config>) en la consola. Si no aparece el indicador, pulse **Intro** de nuevo.

2. Entre el mandato **list devices** para visualizar los números de las interfaces de red que están configuradas actualmente.
3. Anote los números de interfaz.
4. Cree una interfaz de canal de una de las dos formas siguientes:

- Entrando el mandato **add device esc** en el indicador Config> para crear un canal ESCON.

```
Config> add dev esc
Device Slot x(1-8) 1?
Adding ESCON Adapter device in slot 1 port 1 as interface x
```

Nota: x es el número de interfaz asignado.

Nota: El 2216 tiene ocho ranuras, numeradas del 1 al 8.

- Entrando el mandato **add device pca** en el indicador Config>.

```
Config> add dev pca
Device Slot x(1-8) 1?
Adding PCA device in slot 1 port 1 as interface x
```

Nota: x es el número de interfaz asignado.

Nota: El 2216 tiene ocho ranuras, numeradas del 1 al 8.

5. Entre el mandato **network** y el número de la interfaz obtenido en el paso 4. Por ejemplo, si la interfaz 0 es una interfaz ESCON:

```
Config> network 0
ESCON Config>
```

Se visualiza el indicador de configuración ESCON (ESCON Config>).

6. Configure los manejadores de red virtual de adaptador de canal y los subcanales asociados utilizando los mandatos de la Tabla 52.

Mandatos de configuración de adaptador de canal

Los mandatos siguientes se pueden entrar en un indicador de configuración de adaptador de canal (ESC Config> o PCA Config>):

Tabla 52. Mandatos de configuración de interfaz de canal

Mandato	Descripción
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página 10.
add	Añade un manejador de red virtual para uno de los protocolos base o añade un bucle de retorno APPN: <ul style="list-style-type: none"> • LCS - Soporte de Estación de canal de LAN • LSA - Link Services Architecture • MPC+ - Canal de diversas vías de acceso+ • Bucle de retorno APPN Cada protocolo proporciona un conjunto exclusivo de parámetros que se pueden utilizar para configurar los manejadores de red virtual.
delete	Suprime una interfaz de adaptador de canal.
list	Lista la configuración de adaptador de canal y, opcionalmente, lista los subcanales. También puede listar la modalidad de transferencia y la velocidad de transferencia de canal para un PCA.
mod	Cambia la configuración de una interfaz de adaptador de canal.
set	Establece la modalidad de transferencia y la velocidad de transferencia de canal para un adaptador de canal paralelo (PCA). <p>Nota: Sólo se puede acceder a este mandato cuando se configura una interfaz PCA.</p>
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página 11.

Add

Utilice el mandato **add** para añadir manejadores de red virtual para LCS, LSA y MPC+ y para habilitar el bucle de retorno para APPN.

Sintaxis:

```
add                lcs
                  lsa
                  mpc
                  appn loopback
```

Configuración de una interfaz virtual LCS

Utilice el mandato **add lcs** para añadir una interfaz virtual LCS y obtener el indicador ESCON Add Virtual> o PCA Add Virtual> desde el cual puede entrar otros parámetros de interfaz y de subcanal.

Nota: Aunque LCS necesite dos subcanales, sólo es necesario especificar un subcanal. Se elegirá un subcanal adyacente de manera que los dos subcanales formen un par secuencial con el subcanal de grabación (la dirección de dispositivo es par) antes del canal de lectura (la dirección de dispositivo es impar).

Después de entrar **add lcs**, recibirá el indicador ESCON Add Virtual> o PCA Add Virtual>. En este indicador puede entrar los mandatos siguientes:

Mandato	Descripción
---------	-------------

<u>acklen</u> <i>bytes</i>	El tamaño (en bytes) de las tramas de reconocimiento en esta interfaz.
-----------------------------------	--

Nota: El valor por omisión 10 hace que se agrupen en bloques las tramas de reconocimiento. Este valor proporciona el mejor rendimiento en redes de tráfico pesado si se utiliza con el valor por omisión de **blktimer**. Para el tráfico interactivo y la transferencia de datos generales IP, establezca **acklen** en 100.

Valores válidos: De 1 a 500 bytes

Valor por omisión: 10

<u>blktimer</u> <i>milisegundos</i>	El tiempo máximo (en milisegundos) que se ha de esperar antes de enviar un bloque de datos incompleto al sistema principal.
--	---

El tiempo máximo (en milisegundos) que se ha de esperar antes de enviar un bloque de datos incompleto al sistema principal.

Nota: Se establece el valor por omisión para proporcionar el mejor rendimiento en redes de tráfico pesado. Establezca **blktimer** en 10 para el tráfico interactivo y la transferencia de datos generales IP.

Valores válidos: De 1 a 20

Valor por omisión: 5

<u>lantype</u> <i>tipo</i>	El tipo de LAN, que puede ser Ethernet, Red en Anillo o FDDI.
-----------------------------------	---

Mandatos de configuración de adaptador de canal (Talk 6)

Ejemplo: Especificación del Tipo de LAN para una interfaz LCS de una interfaz ESCON

```
ESCON Add Virtual>lan
Please select one of the following LAN types:
  E Ethernet
  T Token Ring
  F FDDI
LCS LAN Type: [E]?
```

mac *dirección* La dirección MAC del manejador de red virtual

maxdata *bytes*

Tamaño máximo de datos manejados por este manejador de red virtual.

Valores válidos: De 516 a 17749 para Red en Anillo, 1500 para Ethernet, 4478 para FDDI

Valores por omisión: 2052 para Red en Anillo, 1500 para Ethernet, 4478 para FDDI

subchannels *mandato*

Le lleva al siguiente indicador basándose en el valor del *mandato*. El *mandato* puede ser uno de los siguientes:

- add
- list
- mod

Consulte la sección “Configuración de un subcanal LCS” para ver los mandatos que puede entrar en estos indicadores y sus descripciones.

enable 3172 emulation

Habilita el Paso a través LCS para permitir que el dispositivo funcione como sustituto de 3172 en redes TCP/IP. Cuando habilita la emulación 3172, se dispone del siguiente menú en el indicador de mandatos ESCON Add Virtual>:

```
ESCON Add Virtual>?
BLKtimer
ACKlen
SUBchannels
DISable 3172 Emulation
NET link
Exit
ESCON Add Virtual>
```

Consulte la sección “Emulación 3172 utilizando el Paso a través LCS” en la página 393 para ver un ejemplo de emulación 3172.

Configuración de un subcanal LCS

Si se entra subchannels *mandato* le lleva al siguiente indicador basándose en el valor del *mandato*. El *mandato* puede ser uno de los siguientes:

- add
- list
- mod
- exit

Mandato

Descripción

add

Añade un par de subcanales y visualiza el indicador ESCON Config LCS Subchannel> o PCA Config LCS Subchannel> desde el cual puede añadir la Dirección de dispositivo, el número de LPAR, la Dirección de enlace y la Dirección lógica de CU.

Mandatos de configuración de adaptador de canal (Talk 6)

Notas:

1. Sólo necesita especificar la dirección de dispositivo para las interfaces PCA.
2. Debe añadir o configurar un subcanal para una interfaz virtual LCS. Aunque LCS necesite dos subcanales, sólo es necesario especificar un subcanal. Se elegirá un subcanal adyacente de manera que los dos subcanales formen un par secuencial con el subcanal de grabación (la dirección de dispositivo es par) antes del canal de lectura (la dirección de dispositivo es impar).

device *dirección*

La dirección de unidad transmitida en la vía de acceso del canal para seleccionar un dispositivo 2216. También se hace referencia como número de subcanal en la arquitectura de E/S S/370. Es un valor hexadecimal de dos dígitos que está en el rango de X'00' a X'FF'. Este valor se define en el IOCP del sistema principal por la sentencia UNITADD en la macroinstrucción CNTLUNIT para el dispositivo real.

Valores válidos: De X'00' a X'FF'

Valor por omisión: Ninguno

Importante

Los parámetros siguientes no se aplican a PCA.

lpar *número*

Número de partición lógica. Permite que múltiples particiones lógicas del sistema principal (LPAR) compartan un canal ESCON.

Este valor se define en el Programa de configuración de la entrada/salida (IOCP) por la macroinstrucción RESOURCE.

Si el sistema principal no utiliza EMIF, utilice el valor por omisión 0 para el número de LPAR.

Valores válidos: De X'0' a X'F'

Valor por omisión: X'0'

link *dirección*

Si hay un Director ESCON (ESCD) en la vía de acceso de comunicación, la dirección del enlace es el número de puerto ESCD que está conectado al sistema principal.

Si hay dos ESCD en la vía de acceso, es el número de puerto de la parte del sistema principal del ESCD definido con la conexión dinámica.

Cuando no hay ningún ESCD en la vía de acceso de comunicación, este valor debe establecerse en X'01'.

Valores válidos: De X'01' a X'0F'

Valor por omisión: X'01'

cu *dirección*

La dirección de la Unidad de control definida en el sistema principal para el 2216. Este valor se define en el Programa

Mandatos de configuración de adaptador de canal (Talk 6)

de configuración de la entrada/salida (IOCP) por la sentencia CUADD en la macroinstrucción CNTLUNIT.

Valores válidos: De X'0' a X'F'

Valor por omisión: X'0'

Ejemplo: Adición de un subcanal para una interfaz LCS para una interfaz ESCON

```
ESCON Add Virtual>sub add
Please add or configure one subchannel for an LCS virtual interface.
Although LCS requires two subchannels, it is only necessary to specify
one subchannel. An adjacent subchannel will be chosen such that the two
subchannels will form a sequential pair with the write subchannel (device
address is even) before the read subchannel (device address is odd).
ESCON Config LCS Subchannel>d 4
ESCON Config LCS Subchannel>e
```

list

Lista la información de los subcanales LCS.

Ejemplo: Listado de subcanales para una interfaz LCS ESCON

```
ESCON Add Virtual>sub lis
Read Subchannels:
Sub 0 Device address : 5 LPAR number : 0
Link address : 1 CU Logical Address : 0
Write Subchannels:
Sub 1 Device address : 4 LPAR number : 0
Link address : 1 CU Logical Address : 0
```

Ejemplo: Listado de subcanales para una interfaz LCS PCA

```
PCA Add Virtual>sub lis
Read Subchannels:
Sub 2 Device address : 3
Write Subchannels:
Sub 3 Device address : 2
```

mod

Modifica un par de subcanales LCS configurados. Lista la configuración para los subcanales LCS configurados y le permite modificar uno de ellos especificando el número de "sub" de la lista. Cuando haya seleccionado el subcanal, puede cambiar la dirección de dispositivo, el número de LPAR, la Dirección de enlace y la Dirección lógica CU, tal como se describe en la sección "Configuración de un subcanal LCS" en la página 412.

Notas:

1. Sólo puede cambiar la dirección de dispositivo para PCA.
2. Para ESCON o PCA, si sólo hay un subcanal configurado, sólo puede modificar el subcanal, no suprimirlo.

Configuración de una interfaz virtual LSA

Utilice el mandato **add lsa** para añadir una interfaz virtual LSA y obtener el indicador ESCON Add Virtual> o PCA Add Virtual> en el que puede entrar los mandatos siguientes:

Mandato	Descripción
----------------	--------------------

[enable o disable]	
---------------------------	--

Habilita o inhabilita el bucle de retorno en una interfaz LSA.

Nota: Sólo puede entrarse **uno** de estos parámetros, dependiendo del estado de la función de bucle de retorno. Si el bucle de retorno está inhabilitado, puede habilitarlo; si está habilitado, puede inhabilitarlo.

Valores válidos: enable o disable

Mandatos de configuración de adaptador de canal (Talk 6)

Valor por omisión: disable

acklen bytes El tamaño (en bytes) de las tramas de reconocimiento en esta interfaz.

Nota: El valor por omisión 10 hace que se agrupen en bloques las tramas de reconocimiento. Este valor proporciona el mejor rendimiento en redes de tráfico pesado si se utiliza con el valor por omisión de **blktimer**. Establezca **acklen** en 100 para la transferencia de datos generales y tráfico interactivo IP.

Valores válidos: De 1 a 500 bytes

Valor por omisión: 10

blktimer milisegundos

El tiempo máximo (en milisegundos) que se ha de esperar antes de enviar un bloque de datos incompleto al sistema principal.

Nota: Se establece el valor por omisión para proporcionar el mejor rendimiento en redes de tráfico pesado. Establezca **blktimer** en 10 para la transferencia de datos generales y el tráfico interactivo IP en las LAN Ethernet y de Red en Anillo.

Valores válidos: De 1 a 20

Valor por omisión: 10

lantype tipo El tipo de LAN, que puede ser Ethernet o Red en Anillo.

mac dirección Una dirección MAC exclusiva para identificar esta interfaz virtual. Este parámetro sólo está disponible cuando está habilitado el bucle de retorno. Se trata de la dirección MAC de la parte LSA/VTAM de la conexión de bucle de retorno. La dirección MAC de la parte APPN de la conexión del bucle de retorno se especifica utilizando ADD APPN.

maxdata bytes

Tamaño máximo de datos manejados por este manejador de red virtual.

Valores válidos: De 516 a 17749 para Red en Anillo, 1500 para Ethernet

Valor por omisión: 2052 para Red en Anillo, 1500 para Ethernet

net númerointerfaz

Este parámetro sólo está disponible cuando el bucle de retorno está inhabilitado. Se utiliza para indicar el adaptador LAN a través del que se comunicará esta red LSA. El adaptador LAN debe haber sido configurado previamente y sólo puede ser Red en Anillo, Ethernet (incluyendo LAN emuladas) o FDDI.

subchannels Le lleva al siguiente indicador basándose en el valor del *mandato*. El *mandato* puede ser uno de los siguientes:

- add
- delete
- list

Mandatos de configuración de adaptador de canal (Talk 6)

- `mod`

Consulte la sección “Configuración de un subcanal LSA” para ver los mandatos que puede entrar en estos indicadores y sus descripciones.

Hay cuatro tipos de conexiones LSA, tal como se muestra en la Figura 26 en la página 394. Son:

- “Configuración de una conexión LSA directa en el 2216” en la página 395
- “Configuración de una conexión LSA APPN en el 2216” en la página 396
- “Configuración de una conexión LSA DLSw en el 2216” en la página 397
- “Configuración de una conversión local LSA DLSw en el 2216” en la página 399

El ejemplo muestra la adición de dos interfaces LSA. La primera utiliza el bucle de retorno y la segunda es una conexión directa.

Ejemplo 1: Adición de una interfaz LSA ESCON con bucle de retorno

```
ESCON Config>add lsa
ESCON Add Virtual>enable
Enabling loopback through network 2.
Please set the MAC address using the "MAC" command
ESCON Add Virtual>mac 40:00:00:00:22:16
ESCON Add Virtual>lan
Please select one of the following LAN types:
  E Ethernet
  T Token Ring
LSA LAN Type: [E]? e
ESCON Add Virtual>sub add
ESCON Add LSA Subchannel>link c5
ESCON Add LSA Subchannel>d 8
ESCON Add LSA Subchannel>e
ESCON Add Virtual>e
ESCON Config>list all
Net: 2 Protocol: LSA LAN type: LSA Ethernet LAN number: 0
      Maxdata: 1500
      Loopback is enabled.
      MAC address: 400000002216
      Block timer: 10 ms ACK length: 10 bytes
      Sub 0 Dev addr: 8 LPAR: 0 Link addr: C5 CU addr: 0
```

Ejemplo 2: Adición de una interfaz LSA PCA con conexión directa

```
PCA Config>add lsa
PCA Add Virtual>net 0
PCA Add Virtual>sub add
PCA Add LSA Subchannel>d 7
PCA Add LSA Subchannel>e
PCA Add Virtual>e
PCA Config>list all
Net: 6 Protocol: LSA LAN type: Token Ring LAN number: 0
      Maxdata: 2052
      Loopback is not enabled.
      MAC address: Obtained from net 0
      Block timer: 10 ms ACK length: 10 bytes
      Sub 0 Dev addr: 7
PCA Config>
```

Configuración de un subcanal LSA

Si se entra **subchannels** *mandato* le lleva al siguiente indicador basándose en el valor del *mandato*. El *mandato* puede ser uno de los siguientes:

- `add`
- `delete`
- `list`
- `mod`
- `exit`

Mandato	Descripción
---------	-------------

Mandatos de configuración de adaptador de canal (Talk 6)

add

Añade un subcanal y visualiza el indicador ESCON Add LSA Subchannel> o PCA Add LSA Subchannel> desde el cual puede añadir:

device *dirección*

La dirección de unidad transmitida en la vía de acceso del canal para seleccionar un dispositivo 2216. También se hace referencia como número de subcanal en la arquitectura de E/S S/370. Es un valor hexadecimal de dos dígitos en el rango de 00 a FF. Este valor se define en el IOCP del sistema principal por la sentencia UNITADD en la macroinstrucción CNTLUNIT para el dispositivo real.

Valores válidos: De X'00' a X'FF'

Valor por omisión: Ninguno

Importante

Los parámetros siguientes no se aplican a PCA.

lpar *número*

Número de partición lógica. Permite que múltiples particiones lógicas del sistema principal (LPAR) compartan un canal ESCON.

Este valor se define en el Programa de configuración de la entrada/salida (IOCP) por la macroinstrucción RESOURCE.

Si el sistema principal no utiliza EMIF, utilice el valor por omisión 0 para el número de LPAR.

Valores válidos: De X'0' a X'F'

Valor por omisión: X'0'

link *dirección*

Si hay un Director ESCON (ESCD) en la vía de acceso de comunicación, la dirección del enlace es el número de puerto ESCD que está conectado al sistema principal.

Si hay dos ESCD en la vía de acceso, es el número de puerto de la parte del sistema principal del ESCD definido con la conexión dinámica.

Cuando no hay ningún ESCD en la vía de acceso de comunicación, este valor debe establecerse en X'01'.

Valores válidos: De X'01' a X'FE'

Valor por omisión: X'01'

cu *dirección*

La dirección de la Unidad de control definida en el sistema principal para el 2216. Este valor se define en el Programa de configuración de la entrada/salida (IOCP) por la sentencia CUADD en la macroinstrucción CNTLUNIT.

Valores válidos: De X'0' a X'F'

Valor por omisión: X'0'

Entre **exit** para volver al indicador anterior.

Mandatos de configuración de adaptador de canal (Talk 6)

Ejemplo: Adición de un subcanal para una interfaz LSA ESCON

```
ESCON Add Virtual>sub add
ESCON Add LSA Subchannel>link f7
ESCON Add LSA Subchannel>device 0
ESCON Add LSA Subchannel>cu 0
ESCON Add LSA Subchannel>lpar 0
ESCON Add LSA Subchannel>exit
```

Ejemplo: Adición de un subcanal para una interfaz LSA PCA

```
PCA Add Virtual>sub add
PCA Add LSA Subchannel>device 2
PCA Add LSA Subchannel>exit
```

delete

Suprime un subcanal LSA configurado. Lista la configuración para los subcanales LSA configurados y le permite suprimir uno de ellos especificando el número de “sub” de la lista.

list

Lista la información para los subcanales LSA.

Ejemplo: Listado de subcanales para una interfaz LSA ESCON

```
ESCON Config Virtual>sub list
Sub 0 Device address : 42 LPAR number : 0
      Link address : C5 CU Logical Address : 0
Sub 1 Device address : 43 LPAR number : 0
      Link address : C5 CU Logical Address : 0
Sub 2 Device address : 44 LPAR number : 0
      Link address : C5 CU Logical Address : 0
```

Ejemplo: Listado de subcanales para una interfaz LSA PCA

```
PCA Config Virtual>sub list
Sub 0 Device address : B
Sub 1 Device address : 12
Sub 2 Device address : 10
Sub 3 Device address : A
Sub 4 Device address : C
Sub 5 Device address : E
```

mod

Modifica un subcanal LSA configurado. Lista la configuración para los subcanales LSA configurados y le permite modificar uno de ellos especificando el número de “sub” de la lista. Cuando haya seleccionado el subcanal, puede cambiar la dirección de dispositivo, el número de LPAR, la Dirección de enlace y la Dirección lógica CU, tal como se describe en la sección “Configuración de un subcanal LSA” en la página 416.

Notas:

1. Sólo puede cambiar la dirección de dispositivo para PCA.
2. Para ESCON o PCA, si sólo hay un subcanal configurado, sólo puede modificar el subcanal, no suprimirlo.

Configuración de una interfaz virtual MPC+

Utilice el mandato **add mpc** para añadir una interfaz virtual MPC+ y obtener el indicador `ESCON Add Virtual>` o `PCA Add Virtual>` desde el que puede entrar otros parámetros de subcanal y de interfaz:

Mandato Descripción

acklen bytes El tamaño (en bytes) de las tramas de reconocimiento en esta interfaz.

Nota: El valor por omisión 10 hace que se agrupen en bloques las tramas de reconocimiento. Este valor proporciona el mejor rendimiento en redes de tráfico pesado si se utiliza con el valor por omisión de `blktimer`.

Valores válidos: De 1 a 500 bytes

Mandatos de configuración de adaptador de canal (Talk 6)

Valor por omisión: 10

blktimer *milisegundos*

El tiempo máximo (en milisegundos) que se ha de esperar antes de enviar un bloque de datos incompleto al sistema principal.

Nota: Se establece el valor por omisión para proporcionar el mejor rendimiento en redes de tráfico pesado.

Valores válidos: De 1 a 20

Valor por omisión: 5

disable_outbound protocol blocking

Impide que el Grupo MPC+ agrupe en bloques varios paquetes de protocolo en un solo paquete MPC+ cuando envía datos al sistema principal.

Nota: Este parámetro afecta al tráfico UDP+ y TCP/IP. La habilitación de este parámetro proporciona un mejor rendimiento en las redes de tráfico pesado. El valor por omisión es habilitado.

disable udp+ exclusive use

Para hacer que la interfaz MPC+ deje de estar dedicada a UDP+.

Notas:

1. Este parámetro sólo se aplica a interfaces ESCON.
2. Esto significa que sólo HPDT UDP del sistema principal podrá establecer una conexión mediante este Grupo MPC+. UDP+ nunca puede compartir un Grupo MPC+ con otros protocolos (por ejemplo, APPN, TCP/IP).

enable_outbound protocol blocking

Permite que el Grupo MPC+ agrupe en bloques varios paquetes de protocolo en un solo paquete MPC+ cuando envía datos al sistema principal.

Nota: Este parámetro afecta al tráfico UDP+ y TCP/IP. La habilitación de este parámetro proporciona un mejor rendimiento en las redes de tráfico pesado. El valor por omisión es habilitado.

enable udp+ exclusive use

Para dedicar la interfaz MPC+ a UDP+.

Notas:

1. Este parámetro sólo se aplica a interfaces ESCON.
2. Esto significa que sólo HPDT UDP del sistema principal podrá establecer una conexión mediante este Grupo MPC+. UDP+ nunca puede compartir un Grupo MPC+ con otros protocolos (por ejemplo, APPN, TCP/IP).

maxdata *bytes*

Tamaño máximo de datos manejados por este manejador de red virtual.

Valores válidos: De 512 a 32 768

Valor por omisión: 2 048

Mandatos de configuración de adaptador de canal (Talk 6)

reply timeout *milisegundos*

Temporizador para el tiempo de espera excedido de XID2/Desconexión en milisegundos.

Valores válidos: De 1 a 50 000

Valor por omisión: 45 000

sequencing interval timer *milisegundos*

Temporizador de secuencia de intervalos en milisegundos.

Valores válidos: De 1 a 50 000

Valor por omisión: 3000

subchannels Le lleva al siguiente indicador basándose en el valor del *mandato*. El *mandato* puede ser uno de los siguientes:

- addr
- addw
- delete
- list
- mod
- exit

Consulte la sección “Configuración de un subcanal MPC+” para ver los mandatos que puede entrar y su descripción.

Configuración de un subcanal MPC+

Nota: Un subcanal definido como un subcanal de lectura en VTAM es un subcanal de grabación en el 2216 y un subcanal definido como un subcanal de grabación en VTAM es un subcanal de lectura para el 2216.

Si se entra subchannels *mandato* le lleva al siguiente indicador basándose en el valor del *mandato*. El *mandato* puede ser uno de los siguientes:

- addr
- addw
- delete
- list
- mod
- exit

Mandatos	Descripción
----------	-------------

<u>addr</u>	Añade un subcanal de lectura y visualiza el indicador ESCON Add MPC+ Read Subchannel> o PCA Add MPC+ Read Subchannel> desde el cual puede entrar los mandatos siguientes:
-------------	---

Mandato	Descripción
---------	-------------

<u>device</u> <i>dirección</i>	La dirección de unidad transmitida en la vía de acceso del canal para seleccionar un dispositivo 2216. También se hace referencia como número de subcanal en la arquitectura de E/S S/370. Es un valor hexadecimal de dos dígitos en el rango de 00 a FF. Este valor se define en el IOCP del sistema
--------------------------------	---

Mandatos de configuración de adaptador de canal (Talk 6)

principal por la sentencia UNITADD en la macroinstrucción CNTLUNIT para el dispositivo real.

Valores válidos: De X'00' a X'FF'

Valor por omisión: Ninguno

Importante

Los parámetros siguientes no se aplican a PCA.

lpar número Número de partición lógica. Permite que múltiples particiones lógicas del sistema principal (LPAR) compartan un canal ESCON.

Este valor se define en el Programa de configuración de la entrada/salida (IOCP) por la macroinstrucción RESOURCE.

Si el sistema principal no utiliza EMIF, utilice el valor por omisión 0 para el número de partición lógica.

Valores válidos: De X'0' a X'F'

Valor por omisión: X'0'

link dirección Si hay un Director ESCON (ESCD) en la vía de acceso de comunicación, la dirección de enlace es el número de puerto ESCD que está conectado al sistema principal.

Si hay dos ESCD en la vía de acceso, es el número de puerto de la parte del sistema principal del ESCD definido con la conexión dinámica.

Cuando no hay ningún ESCD en la vía de acceso de comunicación, este valor debe establecerse en X'01'.

Valores válidos: De X'01' a X'FE'

Valor por omisión: X'01'

cu dirección La dirección de la Unidad de control definida en el sistema principal para el 2216. Este valor se define en el Programa de configuración de la entrada/salida (IOCP) por la sentencia CUADD en la macroinstrucción CNTLUNIT.

Valores válidos: De X'0' a X'F'

Valor por omisión: X'0'

Entre **exit** para volver al indicador ESCON Add Virtual>.

Ejemplo: Adición de subcanales de lectura para una interfaz MPC+ PCA

Mandatos de configuración de adaptador de canal (Talk 6)

```
PCA Add Virtual>sub addr
PCA Add MPC+ Read Subchannel>d 8
PCA Add MPC+ Read Subchannel>e
PCA Add Virtual>sub addr
PCA Add MPC+ Read Subchannel>d 9
PCA Add MPC+ Read Subchannel>e
```

addw

Añade un subcanal de grabación y visualiza el indicador ESCON Add MPC+ Write Subchannel> o PCA Add MPC+ Write Subchannel> desde el que puede entrar los mandatos siguientes:

Mandato	Descripción
---------	-------------

<u>device</u> <i>dirección</i>	
--------------------------------	--

La dirección de unidad transmitida en la vía de acceso del canal para seleccionar un dispositivo 2216. También se hace referencia como número de subcanal en la arquitectura de E/S S/370. Es un valor hexadecimal de dos dígitos en el rango de 00 a FF. Este valor se define en el IOCP del sistema principal por la sentencia UNITADD en la macroinstrucción CNTLUNIT para el dispositivo real.

Valores válidos: De X'00' a X'FF'

Valor por omisión: Ninguno

Importante

Los parámetros siguientes no se aplican a PCA.

<u>lpar</u> <i>número</i>	
---------------------------	--

Número de partición lógica. Permite que múltiples particiones lógicas del sistema principal (LPAR) compartan un canal ESCON.

Este valor se define en el Programa de configuración de la entrada/salida (IOCP) por la macroinstrucción RESOURCE.

Si el sistema principal no utiliza EMIF, utilice el valor por omisión 0 para el número de LPAR.

Valores válidos: De X'0' a X'F'

Valor por omisión: X'0'

<u>link</u> <i>dirección</i>	
------------------------------	--

Si hay un Director ESCON (ESCD) en la vía de acceso de comunicación, la dirección del enlace es el número de puerto ESCD que está conectado al sistema principal.

Si hay dos ESCD en la vía de acceso, es el número de puerto de la parte del sistema principal del ESCD definido con la conexión dinámica.

Cuando no hay ningún ESCD en la vía de acceso de comunicación, este valor debe establecerse en X'01'.

Valores válidos: De X'01' a X'FE'

Valor por omisión: X'01'

Mandatos de configuración de adaptador de canal (Talk 6)

cu dirección La dirección de la Unidad de control definida en el sistema principal para el 2216. Este valor se define en el Programa de configuración de la entrada/salida (IOCP) por la sentencia CUADD en la macroinstrucción CNTLUNIT.

La Dirección de unidad de control debe ser exclusiva para cada partición lógica definida en el mismo sistema principal.

Valores válidos: De X'0' a X'F'

Valor por omisión: X'0'

Ejemplo: Adición de subcanales de grabación para una interfaz MPC+ ESCON

```
ESCON Add Virtual>sub addw
ESCON Add MPC+ Write Subchannel>d 10
ESCON Add MPC+ Write Subchannel>e
ESCON Add Virtual>sub addw
ESCON Add MPC+ Write Subchannel>d 11
ESCON Add MPC+ Write Subchannel>e
```

delete

Suprime un subcanal MPC+ configurado. Lista la configuración para los subcanales MPC+ configurados y le permite suprimir uno de ellos especificando el número de “sub” de la lista.

list

Lista la información para los subcanales MPC+.

Ejemplo: Listado de subcanales para una interfaz MPC+ ESCON

```
ESCON Add Virtual>sub lis
Read Subchannels:
Sub 0 Device address : 8 LPAR number : 0
      Link address  : 1 CU Logical Address : 0
Sub 1 Device address : 9 LPAR number : 0
      Link address  : 1 CU Logical Address : 0
Write Subchannels:
Sub 2 Device address : 10 LPAR number : 0
      Link address  : 1 CU Logical Address : 0
Sub 3 Device address : 11 LPAR number : 0
      Link address  : 1 CU Logical Address : 0
```

Ejemplo: Listado de subcanales para una interfaz MPC+ PCA

```
PCA Add Virtual>sub lis
Read Subchannels:
Sub 0 Device address : 12
Sub 1 Device address : 13
Write Subchannels:
Sub 2 Device address : 14
Sub 3 Device address : 15
```

mod

Modifica un subcanal MPC+ configurado. Lista la configuración para los subcanales MPC+ configurados y le permite modificar uno de ellos especificando el número de “sub” de la lista. Cuando haya seleccionado el subcanal, puede cambiar la dirección de dispositivo, el número de LPAR, la Dirección de enlace y la Dirección lógica CU, tal como se describe en la sección “Configuración de un subcanal MPC+” en la página 420.

Nota: Sólo puede cambiar la dirección de dispositivo para PCA.

Una vez haya vuelto al indicador anterior, puede listar toda la configuración MPC+ tal como se muestra en el ejemplo siguiente:

Ejemplo: Listado y cambio de una configuración MPC+ ESCON

Mandatos de configuración de adaptador de canal (Talk 6)

```
ESCON Config>list all
Net: 1 Protocol: MPC+ LAN type: MPC+ LAN number: 0
Maxdata: 2048
Reply TO: 45000 Sequencing Interval Timer: 3000
MPC Group is for exclusive use of UDP+
Outbound protocol data blocking is enabled
Block timer: 5 ms ACK Length: 10 bytes
Read Subchannels:
Sub 0 Dev addr: 40 LPAR: 0 Link addr: F5 CU addr: 0
Write Subchannels:
Sub 1 Dev addr: 41 LPAR: 0 Link addr: F5 CU addr: 0

Net: 2 Protocol: MPC+ LAN type: MPC+ LAN number: 1
Maxdata: 2048
Reply TO: 45000 Sequencing Interval Timer: 3000
Outbound protocol data blocking is enabled
Block timer: 5 ms ACK Length: 10 bytes
Read Subchannels:
Sub 0 Dev addr: 42 LPAR: 0 Link addr: F5 CU addr: 0
Write Subchannels:
Sub 1 Dev addr: 43 LPAR: 0 Link addr: F5 CU addr: 0

Net: 3 Protocol: MPC+ LAN type: MPC+ LAN number: 2
Maxdata: 2048
Reply TO: 45000 Sequencing Interval Timer: 3000
Outbound protocol data blocking is enabled
Block timer: 5 ms ACK Length: 10 bytes
Read Subchannels:
Sub 0 Dev addr: 44 LPAR: 0 Link addr: F5 CU addr: 0
Write Subchannels:
Sub 1 Dev addr: 45 LPAR: 0 Link addr: F5 CU addr: 0

ESCON Config>mod 3
ESCON Config Virtual> ?
REply timeout
SEQuencing int timer
MAXdata
SUBchannels
Exit
ESCON Config Virtual>rep 3100
ESCON Config Virtual> exit
ESCON Config>list all
Net: 1 Protocol: MPC+ LAN type: MPC+ LAN number: 0
Maxdata: 2048
Reply TO: 45000 Sequencing Interval Timer: 3000
MPC Group is for exclusive use of UDP+
Outbound protocol data blocking is enabled
Block timer: 5 ms ACK Length: 10 bytes
Read Subchannels:
Sub 0 Dev addr: 40 LPAR: 0 Link addr: F5 CU addr: 0
Write Subchannels:
Sub 1 Dev addr: 41 LPAR: 0 Link addr: F5 CU addr: 0

Net: 2 Protocol: MPC+ LAN type: MPC+ LAN number: 1
Maxdata: 2048
Reply TO: 45000 Sequencing Interval Timer: 3000
Outbound protocol data blocking is enabled
Block timer: 5 ms ACK Length: 10 bytes
Read Subchannels:
Sub 0 Dev addr: 42 LPAR: 0 Link addr: F5 CU addr: 0
Write Subchannels:
Sub 1 Dev addr: 43 LPAR: 0 Link addr: F5 CU addr: 0

Net: 3 Protocol: MPC+ LAN type: MPC+ LAN number: 2
Maxdata: 2048
Reply TO: 3100 Sequencing Interval Timer: 3000
Outbound protocol data blocking is enabled
Block timer: 5 ms ACK Length: 10 bytes
Read Subchannels:
Sub 0 Dev addr: 44 LPAR: 0 Link addr: F5 CU addr: 0
Write Subchannels:
Sub 1 Dev addr: 45 LPAR: 0 Link addr: F5 CU addr: 0

ESCON Config>
```

Mandatos de configuración de adaptador de canal (Talk 6)

Configuración de un bucle de retorno APPN

Importante: Sólo necesita configurar el bucle de retorno APPN una vez para cada 2216 físico. Si configura el bucle de retorno APPN en un canal ESCON, no necesita habilitarlo en un canal PCA de mismo 2216.

Notas:

1. No se puede añadir el bucle de retorno APPN a menos que se haya habilitado el bucle de retorno en una red virtual LSA, tal como se describe en la sección “Configuración de una interfaz virtual LSA” en la página 414.
2. Solo puede añadir un bucle de retorno APPN una vez a un IBM 2216 determinado.

Utilice el mandato **add appn** para añadir un bucle de retorno APPN. Obtendrá el indicador ESCON Add Virtual> o PCA Add Virtual> en el que puede entrar los mandatos siguientes:

Mandatos	Descripción
----------	-------------

<u>lantype</u> <i>tipo</i>	Ethernet o Red en Anillo
----------------------------	--------------------------

<u>mac</u> <i>dirección</i>	Una dirección MAC exclusiva para identificar la parte APPN de la conexión de bucle de retorno en el 2216. Esta dirección debe ser diferente de la dirección MAC proporcionada a la parte del sistema principal (VTAM) de la conexión de bucle de retorno al configurar la interfaz LSA.
-----------------------------	---

Ejemplo: Adición de bucle de retorno a una interfaz ESCON

```
ESCON Config>add appn
ESCON Add Virtual>
ESCON Add Virtual>lan
Please select one of the following LAN types:
  E Ethernet
  T Token Ring
APPN LAN Type: [T]?
ESCON Add Virtual>mac
MAC address in 00:00:00:00:00:00 form [000000000000]?
  40:00:22:16:00:09
ESCON Add Virtual>e
ESCON Config>li all
Net: 9 Protocol: APPN Loopback LAN type: Token-Ring/802.5
      APPN loopback MAC address: 400022160009

Net: 5 Protocol: LSA LAN type: Token Ring LAN number: 0
      Maxdata: 2052
      Loopback is enabled.
      MAC address: 400022160005
      Block timer: 10 ms ACK length: 10 bytes
      Sub 0 Dev addr: 0 LPAR: 0 Link addr: 1 CU num: 0

Net: 6 Protocol: LSA LAN type: Token Ring LAN number: 1
      Maxdata: 2052
      Loopback is not enabled.
      MAC address: Obtained from net 3
      Block timer: 10 ms ACK length: 10 bytes
      Sub 0 Dev addr: 1 LPAR: 0 Link addr: 1 CU num: 0

Net: 7 Protocol: LCS LAN type: LCS Ethernet 802.3 LAN number: 0
      Maxdata: 1500
      MAC address: 400022160007
      Block timer: 5 ms ACK length: 10 bytes
      Read Subchannels:
      Sub 0 Dev addr: 5 LPAR: 0 Link addr: 1 CU num: 0
      Write Subchannels:
      Sub 1 Dev addr: 4 LPAR: 0 Link addr: 1 CU num: 0
ESCON Config>e
```

Notas:

1. El puerto APPN se reconfiguraría en la red 9 del ejemplo.

Mandatos de configuración de adaptador de canal (Talk 6)

2. Configure las estaciones de enlace APPN que se conectarán a VTAM a través del canal ESCON para que utilicen la dirección MAC de la red LSA como la dirección MAC de destino. No utilice la red de bucle de retorno APPN para esta finalidad.
3. Cualquier conexión de redes LSA con APPN debe tener el mismo tipo de LAN que la red de bucle de retorno APPN.

Delete

Utilice el mandato **delete** para suprimir una interfaz de adaptador de canal. Si conoce el número de interfaz que desea suprimir, puede especificarlo; de lo contrario, si no entra ningún número de interfaz, se lista la configuración y se le solicitará que entre un número de interfaz.

Sintaxis:

delete *número_interfaz*
(sin parámetros)

número_interfaz

Suprime la configuración para el número de interfaz especificado.

(sin parámetros)

Lista las interfaces configuradas para el adaptador de canal y le solicita el número de interfaz que desea suprimir.

Ejemplo: Supresión de una interfaz (sin proporcionar parámetros)

```
PCA Config>de1
Net: 5 Protocol: APPN Loopback LAN type: Token-Ring/802.5
      APPN loopback MAC address: 400000000406
Net: 2 Protocol: LSA LAN type: Token Ring LAN number: 0
      Maxdata: 2052
      Loopback is enabled.
      MAC address: 400000000403
      Block Timer: 10 ms ACK length: 10 bytes
Net: 3 Protocol: LSA LAN type: Token Ring LAN number: 1
      Maxdata: 2052
      Loopback is not enabled.
      MAC address: Obtained from net 1
      Block Timer: 10 ms ACK length: 10 bytes
Net: 4 Protocol: MPC+ LAN type: MPC+ LAN number: 0
      Maxdata: 2048
      Reply TO: 3100 Sequencing Interval Timer: 3000

      Outbound protocol data blocking is enabled
      Block Timer: 5 ms ACK length: 10 bytes
Virtual net number to delete: [2]? 3
Are you sure?(Yes or [No]): y
```

Mod

Utilice el mandato **mod** para modificar una interfaz configurada en el adaptador de canal. Si conoce el número de la interfaz que desea modificar, puede especificarlo; de lo contrario, si no entra ningún número de interfaz, se lista la configuración y se solicita que entre un número de interfaz.

Sintaxis:

modify *número_interfaz*
(sin parámetros)

número_interfaz

Modifica la configuración para el número de interfaz especificado.

Mandatos de configuración de adaptador de canal (Talk 6)

(sin parámetros)

Lista las interfaces configuradas para el adaptador de canal y le solicita el número de interfaz que desea modificar.

Mandatos de configuración de adaptador de canal (Talk 6)

Ejemplo:

```
ESCON Config> mod
Net: 1 Protocol: MPC+ LAN type: MPC+ LAN number: 0
Maxdata: 2048
Reply TO: 45000 Sequencing Interval Timer: 3000
MPC Group is for exclusive use of UDP+
Outbound protocol data blocking is enabled
Block timer: 5 ms ACK length: 10 bytes
Net: 2 Protocol: MPC+ LAN type: MPC+ LAN number: 1
Maxdata: 2048
Reply TO: 45000 Sequencing Interval Timer: 3000
Outbound protocol data blocking is enabled
Block timer: 5 ms ACK length: 10 bytes
Virtual net number to configure: [1]? 2
ESCON Config Virtual> ?
REply timeout
SEQuencing int timer
MAXdata
SUBchannels
Exit
ESCON Config Virtual>re
Reply Time Out (range 1-50000 milliseconds): [45000]? 30003
ESCON Config Virtual>sub list
Read Subchannels:
Sub 0 Device address : 7 LPAR number : 0
Link address : F4 CU Logical Address : 0
Write Subchannels:
Sub 1 Device address : 6 LPAR number : 0
Link address : F4 CU Logical Address : 0
ESCON Config Virtual>sub addr
ESCON Add MPC+ Read Subchannel> ?
LINK address (ESCD Port)
LPAR number
CU logical address
Device address
Exit
ESCON Add MPC+ Read Subchannel>d 5
ESCON Add MPC+ Read Subchannel>? e
ESCON Config Virtual>sub list
Read Subchannels:
Sub 0 Device address : 7 LPAR number : 0
Link address : F4 CU Logical Address : 0
Sub 1 Device address : 5 LPAR number : 0
Link address : F4 CU Logical Address : 0
Write Subchannels:
Sub 2 Device address : 6 LPAR number : 0
Link address : F4 CU Logical Address : 0
ESCON Config Virtual>sub ?
ADDRead subchannel
ADDWrite subchannel
MODify subchannel
DELete subchannel
LIst subchannels
ESCON Config Virtual>sub del
Read Subchannels:
Sub 0 Device address : 7 LPAR number : 0
Link address : F4 CU Logical Address : 0
Sub 1 Device address : 5 LPAR number : 0
Link address : F4 CU Logical Address : 0
Write Subchannels:
Sub 2 Device address : 6 LPAR number : 0
Link address : F4 CU Logical Address : 0
Subchannel number to delete: [0]? 0
Are you sure?(Yes or [No]): y
ESCON Config Virtual>sub list
Read Subchannels:
Sub 0 Device address : 5 LPAR number : 0
Link address : F4 CU Logical Address : 0
Write Subchannels:
Sub 1 Device address : 6 LPAR number : 0
Link address : F4 CU Logical Address : 0
```

Mandatos de configuración de adaptador de canal (Talk 6)

```
ESCON Config Virtual>sub mod
  Read Subchannels:
  Sub 0 Device address : 5 LPAR number : 0
    Link address : F4 CU Logical Address : 0
  Write Subchannels:
  Sub 1 Device address : 6 LPAR number : 0
    Link address : F4 CU Logical Address : 0
Subchannel number to modify: [0]? 1
ESCON Modify MPC+ Subchannel>d 2
ESCON Modify MPC+ Subchannel>e
ESCON Config Virtual>sub list
  Read Subchannels:
  Sub 0 Device address : 5 LPAR number : 0
    Link address : F4 CU Logical Address : 0
  Write Subchannels:
  Sub 1 Device address : 2 LPAR number : 0
    Link address : F4 CU Logical Address : 0
ESCON Config Virtual> exit
ESCON Config>
```

List (ESCON)

Utilice el mandato **list** para listar la configuración de adaptador de canal y también (con **list all**) listar un resumen de los subcanales.

Sintaxis:

list (sin parámetros)

all

(sin parámetros)

Lista la configuración de adaptador de canal.

Ejemplo: Listado de una configuración ESCON

```
ESCON Config>li
Net: 5 Protocol: LSA LAN type: Token Ring LAN number: 0
Maxdata: 2052
Loopback is enabled.
MAC address: 400022160005
Block timer: 10 ms ACK length: 10 bytes
```

all Lista la configuración del canal con un resumen de los subcanales. Se proporcionan tres ejemplos. El primero es para un adaptador de canal con subcanales LSA y LCS. El segundo es para un adaptador de canal con subcanales MPC+. El tercer ejemplo muestra el resultado de la emulación 3172.

Ejemplo para LSA y LCS: Listado de una configuración ESCON con resumen de los subcanales

```
ESCON Config>li all
Net: 2 Protocol: LCS LAN type: LCS FDDI LAN number: 0
Maxdata: 4478
MAC address: 400000002216
Block Timer: 5 ms ACK Length: 10 bytes
Sub 0 Dev addr: 8 LPAR: 0 Link addr: C5 CU addr: 0

Net: 5 Protocol: LSA LAN type: Token Ring LAN number: 0
Maxdata: 2052
Loopback is enabled.
MAC address: 400022160005
Block timer: 10 ms ACK length: 10 bytes
Sub 0 Dev addr: 0 LPAR: 0 Link addr: 1 CU addr: 0
```

Ejemplo con la emulación 3172 habilitada:

```
ESCON Config>list
Net: 5 Protocol: LCS LAN type: Token Ring LAN number: 0
3172 Emulation is enabled.
MAC address: Obtained from net 0
Block Timer: 5 ms ACK length: 10 bytes
ESCON Config>list all
Net: 5 Protocol: LCS LAN type: Token Ring LAN number: 0
3172 Emulation is enabled.
```

Mandatos de configuración de adaptador de canal (Talk 6)

```
MAC address: Obtained from net 0
Block Timer: 5 ms ACK length: 10 bytes
Read Subchannels:
Sub 0 Dev addr: 21 LPAR: 0 Link addr: F7 CU addr: 0
Write Subchannels:
Sub 1 Dev addr: 20 LPAR: 0 Link addr: F7 CU addr: 0
```

ESCON Config>

Ejemplo para MPC+: Listado de una configuración ESCON con resumen de los subcanales

```
Net: 1 Protocol: MPC+ LAN type: MPC+ LAN number: 0
Maxdata: 2048
Reply TO: 45000 Sequencing Interval Timer: 3000
MPC Group is for exclusive use of UDP+
Outbound protocol data blocking is enabled
Block Timer: 5 ms ACK Length: 10 bytes
Read Subchannels:
Sub 0 Dev addr: 40 LPAR: 0 Link addr: F5 CU addr: 0
Write Subchannels:
Sub 1 Dev addr: 41 LPAR: 0 Link addr: F5 CU addr: 0

Net: 2 Protocol: MPC+ LAN type: MPC+ LAN number: 1
Maxdata: 2048
Reply TO: 45000 Sequencing Interval Timer: 3000
Outbound protocol data blocking is enabled
Block Timer: 5 ms ACK Length: 10 bytes
Read Subchannels:
Sub 0 Dev addr: 42 LPAR: 0 Link addr: F5 CU addr: 0
Write Subchannels:
Sub 1 Dev addr: 43 LPAR: 0 Link addr: F5 CU addr: 0
```

List (PCA)

Utilice el mandato **list** para listar la modalidad de transferencia y la velocidad de transferencia de canal configuradas o las interfaces virtuales configuradas.

Sintaxis:

```
list base
virtual
```

base Lista la modalidad de transferencia y la velocidad de transferencia de canal configuradas.

virtual [all o (sin parámetros)]

Lista un resumen de la configuración para las interfaces virtuales o la configuración de todas las interfaces virtuales y sus subcanales (**all**).

Set (sólo PCA)

Utilice el mandato **set** para establecer la modalidad de transferencia y la velocidad de transferencia de canal para un adaptador de canal paralelo (PCA).

Sintaxis:

```
set tmode valor
```

tmode *valor*

Especifica la modalidad de transferencia que el 2216 utiliza para transferir los datos al sistema principal, el interbloqueo DC o la Corriente de datos y la velocidad de transferencia de canal cuando se utiliza la corriente de datos.

Valores válidos:

D Especifica la modalidad de interbloqueo Directo con par (DC). Esta modalidad es la interfaz de E/S estándar que necesita una respuesta a una petición.

Mandatos de configuración de adaptador de canal (Talk 6)

- S** Especifica las velocidades inferiores o iguales a una modalidad de corriente de datos de 3,0 MB.
- S4** Especifica las velocidades inferiores o iguales a una modalidad de corriente de datos de 4,5 MB.

Valor por omisión: D

Acceso al proceso de supervisión de interfaces de canal

Para acceder a la interfaz ESCON o PCA:

1. En el indicador OPCODE, entre **talk 5**. Por ejemplo:

```
* talk 5
+
```

2. Para visualizar el indicador de supervisión para la interfaz de canal o cualquier otra interfaz virtual de adaptador de canal entre el mandato **network** seguido del número de la interfaz.

Si no conoce el número de la interfaz, utilice el mandato **configuration** en el indicador + para visualizar una lista de números de las interfaces configuradas en el direccionador.

Multiprotocol Access Services

2216-MAS Feature 2822 V3.2 Mod 0 PTF 0 RPQ 0 MAS.EF9 cc4_2a

```
Num Name Protocol
0 IP DOD-IP
3 ARP Address Resolution
11 SNMP Simple Network Management Protocol
23 ASRT Adaptive Source Routing Transparent Enhanced Bridge
28 APPN Advanced Peer-to-Peer Networking [HPR]
29 NHRP Next Hop Routing Protocol
30 APPN Advanced Peer-to-Peer Networking [ISR]
```

```
Num Name Feature
2 MCF MAC Filtering
8 NDR Network Dispatching Router
10 AUTH Authentication
```

```
31 Networks:
Net Interface MAC/Data-Link Hardware State
0 TKR/0 Token-Ring/802.5 Token-Ring Up
1 Eth/0 Ethernet/IEEE 802.3 Ethernet Up
2 PCA/0 Parallel Channel Parallel Channel Up
3 LCS/0 LCS Parallel Channel Up
4 MPC/0 MPC Parallel Channel Up
5 LSA/0 LSA Parallel Channel Up
6 TKR/1 Token-Ring/802.5 APPN Loopback Up
7 ESCON/0 ESCON ESCON Channel Up
8 MPC/1 MPC ESCON Channel Up
9 LCS/1 LCS ESCON Channel Up
10 LSA/1 LSA ESCON Channel Up
```

Mandatos de supervisión de interfaces de canal

Los mandatos siguientes se pueden entrar en el indicador de supervisión de adaptador de canal (ESCON> o PCA>):

Tabla 53. Mandatos de supervisión de interfaces de canal

Mandato	Descripción
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado "Cómo obtener ayuda" en la página 10.
List	Lista los subcanales o lista las redes.
Net	Lista una interfaz de red específica.

Mandatos de supervisión de interfaces de canal (Talk 5)

Tabla 53. Mandatos de supervisión de interfaces de canal (continuación)

Mandato	Descripción
Dump_adapter	Toma un vuelco sin interrupciones de la IRAM y DRAM de adaptador de canal.
HIDtrace	Sólo para PCA, activa y desactiva el rastreo HID de adaptador de canal (p. ej., AIB).
Trace	Activa y desactiva los diversos rastreos de microcódigo de adaptador de canal.
Tune	Modifica varios parámetros del manejador de red base.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página 11.

List

Utilice el mandato **list** para listar todos los subcanales o para listar todas las interfaces de red. También puede listar la velocidad de una interfaz PCA.

Sintaxis:

```
list                    base (sólo para PCA)
                        nets
                        subchannels
```

base Lista la modalidad de transferencia y la velocidad de transferencia de canal de adaptador de canal.

nets Lista las interfaces de red.

Ejemplo: Lista de redes

```
PCA>li ne
+ net 1
PCA Base Monitoring
PCA> li nets
Net: 2   Type: LSA   LAN Type: Token-Ring/802.5   LAN Number: 0
         Net state: Up
Net: 4   Type: LSA   LAN Type: Token-Ring/802.5   LAN Number: 1
         Net state: Up
Net: 5   Type: LCS   LAN Type: FDDI               LAN Number: 0
         Net state: Down
```

Type Tipo de la interfaz virtual: LCS, LSA o MPC+

LAN Type

Tipo de LAN, Red en Anillo/802.5, Ethernet/802.3, Ethernet/V2, Ethernet o FDDI.

Nota: Este campo no se visualiza para los subcanales que forman parte de una interfaz MPC+.

LAN Number

El número de interfaz de la LAN

Nota: Este campo no se visualiza para los subcanales que forman parte de una interfaz MPC+.

Group Number

El dispositivo utiliza internamente el número del grupo para identificar una interfaz de red MPC+ virtual en el adaptador de canal.

Mandatos de supervisión de interfaces de canal (Talk 5)

Net State

Estado de la red: Up, Down, Disabled, Not Present, HW Mismatch, o Testing.

Up Indica que el enlace está activado.

Down Indica que el enlace está desactivado.

Disabled

Indica que el operador ha inhabilitado el enlace.

Not Present

Indica que el adaptador de la interfaz de red no está presente.

HW Mismatch

Hay un adaptador que no es de canal en la ranura o el adaptador de canal físico instalado no es del mismo tipo que el adaptador de canal configurado.

Nota: Sólo las redes base tendrán estados “ Not present” y “HW mismatch.”

Testing

El sistema intenta determinar si una conexión de red existe

subchannels

Lista los subcanales

```
ESCON> li su
The following subchannels are defined:
Local address: 00 Device address: 00 CU Logical Address: 00
Link: C5 LPAR: 00
Type: LSA
The following lantypes/lannums are using this subchannel:
LAN type: Token-Ring/802.5 LAN number: 0
Local address: 01 Device address: DD CU Logical Address: 0B
Link: 5C LPAR: 02
Type: LSA
The following lantypes/lannums are using this subchannel:
LAN type: Token-Ring/802.5 LAN number: 0
Local address: 02 Device address: 07 CU Logical Address: 00
Link: C5 LPAR: 00
Type: LSA
The following lantypes/lannums are using this subchannel:
LAN type: Token-Ring/802.5 LAN number: 1
Local address: 03 Device address: 02 CU Logical Address: 00
Link: C5 LPAR: 00
Type: LCS
The following lantypes/lannums are using this subchannel:
LAN type: FDDI LAN number: 0
Local address: 04 Device address: 03 CU Logical Address: 00
Link: C5 LPAR: 00
Type: LCS
The following lantypes/lannums are using this subchannel:
LAN type: FDDI LAN number: 0
```

Local Address

El índice de direcciones de subcanal utilizado internamente por el dispositivo.

Device Address

La dirección de unidad transmitida en la vía de acceso del canal para seleccionar un dispositivo. También se hace referencia como número de subcanal en la arquitectura de E/S S/370. Es un valor hexadecimal de dos dígitos en el rango de X'00' a X'FF'. Este valor se define en el IOCP del sistema principal por la sentencia UNITADD en la macroinstrucción CNTLUNIT para el dispositivo real.

Mandatos de supervisión de interfaces de canal (Talk 5)

Nota: La Dirección lógica CU, la Dirección de enlace y el LPAR sólo se visualizan para adaptadores ESCON.

CU Logical Address

La dirección de Unidad de control definida en el sistema principal para el dispositivo. Este valor se define en el Programa de configuración de la entrada/salida (IOCP) por la sentencia CUADD en la macroinstrucción CNTLUNIT.

La Dirección de unidad de control debe ser exclusiva para cada LPAR definido en el mismo sistema principal.

Link Address

Si hay un Director ESCON (ESCD) en la vía de acceso de comunicación, la dirección del enlace es el número de puerto ESCD que está conectado al sistema principal.

Si hay dos ESCD en la misma vía de acceso, la dirección del enlace es el número de puerto de la parte del sistema principal del ESCD definido con la conexión dinámica.

Cuando no hay ningún ESCD en la vía de acceso de comunicación, este valor debe establecerse en 0x01.

LPAR Número de partición lógica. Permite que múltiples particiones de un sistema principal particionado lógicamente (LPAR) compartan una fibra ESCON.

Este valor se define en el Programa de configuración de la entrada/salida (IOCP) por la macroinstrucción RESOURCE.

Si el sistema principal no utiliza EMIF, el número de LPAR es 0 (cero).

Type Tipo de la interfaz virtual: LCS, LSA o MPC+

LAN Type

Tipo de LAN, Red en Anillo/802.5, Ethernet/802.3, Ethernet/V2, Ethernet o FDDI.

Nota: Este campo no se visualiza para los subcanales que forman parte de una interfaz MPC+.

LAN Number

El número de interfaz de la LAN

Nota: Este campo no se visualiza para los subcanales que forman parte de una interfaz MPC+.

Group Number

El dispositivo utiliza internamente el número del grupo para identificar una interfaz de red MPC+ virtual en el adaptador de canal.

Net

Utilice el mandato **net** para pasar al entorno de supervisión para una de las interfaces virtuales, tal como se describe en:

- "Mandatos de supervisión de interfaces LCS de adaptador de canal" en la página 436
- "Mandatos de supervisión de interfaces LSA de adaptador de canal" en la página 438

Mandatos de supervisión de interfaces de canal (Talk 5)

- "Mandatos de supervisión de interfaces MPC+ de adaptador de canal" en la página 441

Sintaxis:

net *número_red*

Dump_adapter

Utilice el mandato **dump_adapter** para realizar un vuelco sin interrupciones de la IRAM y DRAM de adaptador de canal.

Sintaxis:

dump_adapter

HIDTrace

Sólo para PCA, utilice el mandato **hidtrace** para activar o desactivar el rastreo HID de adaptador de canal (p. ej., AIB).

Sintaxis:

hidtrace

Trace

Utilice el mandato **trace** para activar y desactivar varios rastreos de microcódigo de adaptador de canal.

Sintaxis:

trace *máscara*

máscara

Una máscara de rastreo válida.

Valores válidos: De X'0000' a X'FFFF'

Valores por omisión: Se solicitará el valor de entrada

Nota: X'FFFF' activa todos los rastreos. X'0000' desactiva todos los rastreos.

Tune

Utilice el mandato **tune** para modificar los diversos parámetros del manejador de red base.

Sintaxis:

tune *iplow*

opfair

iplow La marca del nivel mínimo para el control de flujo de la cola de entrada del manejador de red. Consulte el mandato **queue** de GWCON para ver más detalles.

Valores válidos: De 0 a 255

Valores por omisión: Se solicitará el valor de entrada

Mandatos de supervisión de interfaces de canal (Talk 5)

Nota: El manejador de red debe estar desactivado o inhabilitado para actualizar este campo.

opfair El nivel equitativo para la longitud de la cola de salida del manejador de la red. Consulte el mandato queue de GWCON para ver más detalles.

Valores válidos: De 0 a 255

Valores por omisión: Se solicitará el valor de entrada

Nota: El manejador de red debe estar desactivado o inhabilitado para actualizar este campo.

Mandatos de supervisión de interfaces LCS de adaptador de canal

Se pueden entrar los mandatos siguientes en el indicador de supervisión LCS (LCS>):

Tabla 54. Mandatos de supervisión de interfaces LCS de adaptador de canal

Mandato	Descripción
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado "Cómo obtener ayuda" en la página 10.
List	Lista los subcanales o lista las redes.
Tune	Modifica varios parámetros del manejador de red LCS.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página 11.

List

Utilice el mandato **list** para visualizar la información para una interfaz LCS.

Sintaxis:

list

Ejemplo:

```
LCS> list
LCS Virtual Adapter
LCS Information for Net 4
-----
LAN Type: Token-Ring/802.5      LAN Number: 0
Local Read Subchannel number: 7
Local Write Subchannel number: 6
MAC Address: 400022160001
Local IP Address: 9.192.200.1
Tuning Information: ACKLEN= 10, BLKTIMER= 5
Status: Down
```

Ejemplo con la emulación 3172 habilitada

```
LCS> list

LCS Virtual Adapter
LCS Information for Net 5
-----
LAN Type: Token-Ring          LAN Number: 0
Local Read Subchannel number: 1
Local Write Subchannel number: 0
```

Mandatos de supervisión de interfaces de canal (Talk 5)

MAC Address: 08005AFE0144
LCS 3172 Emulation to net 0
Tuning Information: ACKLEN= 10, BLKTIMER= 5
Status: Down

LAN Type

Tipo de LAN, Red en Anillo/802.5, Ethernet/802.3, Ethernet/V2, Ethernet o FDDI.

Nota: Este campo no se visualiza para los subcanales que forman parte de una interfaz MPC+.

LAN Number

El número de interfaz de la LAN

Nota: Este campo no se visualiza para los subcanales que forman parte de una interfaz MPC+.

Read Subchannel

El subcanal local desde el cual el dispositivo recibe los datos.

Write Subchannel

El subcanal local a través del cual el dispositivo transmite los datos.

MAC Address

Una dirección MAC exclusiva para identificar esta interfaz virtual.

Local IP address

Dirección IP que se ha asignado a esta interfaz de red. Si no ha configurado ninguna dirección IP, esta línea no se visualizará.

LCS Bridging

Sólo se visualiza cuando está configurado el puente. (No aparece en el ejemplo.)

Acklen

El tamaño (en bytes) de las tramas de reconocimiento en esta interfaz de red.

Blktimer

El tiempo máximo (en milisegundos) que se ha de esperar antes de enviar un bloque de datos incompleto al sistema principal.

Status

El estado de la red: Up, Down, Disabled, Not Present, HW Mismatch o Testing

Up Se ha establecido la conexión de la red.

Down La conexión de la red no puede determinarse.

Disabled

El dispositivo está inhabilitado y se puede realizar la prueba de diagnóstico

Not Present

Indica que el adaptador de la interfaz de red no está presente.

HW Mismatch

Hay un adaptador que no es de canal en la ranura o el adaptador de canal físico instalado no es del mismo tipo que el adaptador de canal configurado.

Mandatos de supervisión de interfaces de canal (Talk 5)

Nota: Sólo las redes base tendrán estados “ Not present” y “HW mismatch.”

Testing

El sistema intenta determinar si una conexión de red existe

Tune

Utilice el mandato **tune** para modificar varios parámetros del manejador de red LCS.

Sintaxis:

tune acklen
blktimer

acklen

El tamaño (en bytes) de las tramas de reconocimiento de esta interfaz de red LCS.

Valores válidos: De 0 a 500

Valores por omisión: Se solicitará el valor de entrada

Nota: El manejador de red base con el cual está asociado el manejador de red LCS debe estar activado para poder modificar este campo.

blktimer

El tiempo máximo (en milisegundos) que se ha de esperar antes de enviar un bloque de datos incompleto al sistema principal.

Valores válidos: De 0 a 20

Valores por omisión: Se solicitará el valor de entrada

Nota: El manejador de red base con el cual está asociado el manejador de red LCS debe estar activado para poder modificar este campo.

Mandatos de supervisión de interfaces LSA de adaptador de canal

Se pueden entrar los mandatos siguientes en el indicador de supervisión LSA (LSA>):

Tabla 55. Mandatos de supervisión de interfaces LSA de adaptador de canal

Mandato	Descripción
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página 10.
List	Lista información de los adaptadores, los SAP o las estaciones de enlace.
Tune	Modifica varios parámetros del manejador de red LSA.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página 11.

List

Utilice el mandato **list** para visualizar información de los adaptadores, los SAP y las estaciones de enlace.

Sintaxis:

Mandatos de supervisión de interfaces de canal (Talk 5)

list adapter
 sap
 link stations

adapter

Lista los adaptadores virtuales para LSA.

Ejemplo: Lista de adaptadores virtuales para LSA

```
LSA> list ad
LSA Virtual Adapter
LSA Information for Net 2
-----
LAN Type: Token-Ring/802.5        LAN Number: 0
MAC Address: 4000000000CF
Downstream network: Loopback - Net 2
Tuning Information: ACKLEN= 10, BLKTIMER= 10
Status: Host connected
```

```
#SAPs Open: 1        #Link Stations Open: 1
Maximum frame size: 2052 (0x804)
Host User ID                        Subchannel
-----
00000000                            0
```

1 host user(s)

Acklen

El tamaño (en bytes) de las tramas de reconocimiento en esta interfaz de red.

Blktimer

El tiempo máximo (en milisegundos) que se ha de esperar antes de enviar un bloque de datos incompleto al sistema principal.

#SAPs Open

El número de SAP abiertos por VTAM en esta interfaz LSA

#Link Stations Open

Número de estaciones de enlace abiertas para todos los SAP de esta interfaz LSA

Maximum Frame Size

Tamaño máximo de trama soportado en esta interfaz LSA

Host User ID

Un ID exclusivo generado por VTAM para identificar al usuario del sistema principal de un subcanal determinado

Subchannel

El subcanal local que este usuario del sistema principal está utilizando.

sap Lista los puntos de acceso a servicios (SAP) para LSA

Ejemplo: Lista de SAP para LSA

```
LSA> list sap
SAP        Provider        User        Max Link        Open Link
Number     SAP ID        SAP ID     Stations        Stations
-----
4    02000000    00000001        1                1
1 SAPs currently open
```

SAP Number

Identifica el SAP en LLC

Provider SAP ID

Un ID exclusivo generado por VTAM para identificar este SAP

Mandatos de supervisión de interfaces de canal (Talk 5)

User SAP ID

Un ID exclusivo generado por el dispositivo para identificar este SAP

Max Link Stations

Número máximo de estaciones de enlace que VTAM puede abrir en este SAP

Open Link Stations

Número de estaciones de enlace abiertas actualmente en este SAP

link Lista información de enlace para LSA

Ejemplo: Lista de enlaces para LSA

```
LSA> list link
Please specify a SAP number (0-236): [4]? 4
Link Stations on SAP 4
```

Station ID	Destination MAC Address	Destination SAP Number	Link Status	Frames Sent	Frames Received
02000001	40000000ABCD	4	Connected	9	9

1 link station(s) open on SAP 4

Station ID

Un ID exclusivo generado por el dispositivo para identificar esta estación de enlace

Destination MAC Address

Dirección MAC de la estación de enlace LLC remota

Destination SAP Number

Valor SAP de la estación de enlace LLC remota

Link Status

Estado actual de la conexión LLC

Frames Sent

Número de paquetes enviados a VTAM para esta estación de enlace

Frames Received

Número de paquetes recibidos de VTAM para esta estación de enlace

Tune

Utilice el mandato **tune** para modificar varios parámetros del manejador de red LSA.

Sintaxis:

```
tune                acklen
                    blktimer
```

acklen

El tamaño (en bytes) de las tramas de reconocimiento de esta interfaz de red LSA.

Valores válidos: De 0 a 500

Valores por omisión: Se solicitará el valor de entrada

Nota: El manejador de red base con el cual está asociado el manejador de red LSA debe estar activado para poder modificar este campo.

Mandatos de supervisión de interfaces de canal (Talk 5)

blktimer

El tiempo máximo (en milisegundos) que se ha de esperar antes de enviar un bloque de datos incompleto al sistema principal.

Valores válidos: De 0 a 20

Valores por omisión: Se solicitará el valor de entrada

Nota: El manejador de red base con el cual está asociado el manejador de red LSA debe estar activado para poder modificar este campo.

Mandatos de supervisión de interfaces MPC+ de adaptador de canal

Se pueden entrar los mandatos siguientes en el indicador de supervisión MPC+ (MPC+>):

Tabla 56. Mandatos de supervisión de interfaces MPC+ de canal

Mandato	Descripción
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado "Cómo obtener ayuda" en la página 10.
List	Lista los subcanales.
Tune	Modifica varios parámetros del manejador de red MPC+
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página 11.

List

Utilice el mandato **list** para visualizar la información del Grupo MPC+, los subcanales, el Gestor de conexión (CM) y la conexión.

Sintaxis: list cm
connection
mpc group
subchannel

cm Muestra información sobre el Gestor de conexión que está en ejecución en el Grupo MPC+. La información mostrada es la señal del grupo, el tipo del gestor de conexión y el estado actual.

Los estados son:

Reset El CM está inactivo actualmente.

Pending Active-waiting for MPC+ Group

El Grupo MPC+ básico está activándose.

Pending Active-waiting for this side

La otra parte ha iniciado una activación del CM pero esta parte no ha empezado a activar el CM.

Pending Active-waiting for other side

Esta parte ha iniciado una activación del CM pero la otra parte no ha empezado a activar el CM.

Pending Active-callee

Esta parte está esperando que la otra parte, que es el llamador de esta activación inicie la llamada.

Mandatos de supervisión de interfaces de canal (Talk 5)

Pending Active-caller

Esta parte ha llamado a la otra parte y espera que la otra parte responda a la llamada.

Active Activo y utilizable

Ejemplo: Lista de un CM activo para MPC+

```
MPC+>1i cm
MPC+ Connection Managers(CM)
      Group Token      type      state
-----
090144953400000009          PTP Active
```

Ejemplo: Lista de ningún CM activo para MPC+

```
MPC+>1i cm
No CMs on this MPC+ Group
```

connection

Muestra información sobre las conexiones que se ejecutan en el Grupo MPC+/Gestor de conexión. La información mostrada se reparte en dos partes: el circuito virtual y las conexiones bajo el circuito virtual. Se muestra la siguiente información para el circuito virtual: las señales de circuito virtual local y remoto, el tipo de protocolo y el estado actual.

Local Virtual Circuit Token

Señal del dispositivo que representa este circuito virtual.

Remote Virtual Circuit Token

Señal del sistema principal que representa este circuito virtual. Este campo está en blanco si no se conoce.

Protocol

El protocolo de capa superior que este circuito virtual utiliza.

States for the Virtual Circuit

Los estados para el circuito virtual son:

Reset El circuito virtual está inactivo actualmente.

Active-other side

La otra parte está aceptando llamadas (conexiones) actualmente para este circuito virtual.

Active-this side

Esta parte está aceptando llamadas (conexiones) actualmente para este circuito virtual.

Active-both sides

Ambas partes del circuito virtual están aceptando llamadas (conexiones) para este circuito virtual.

Not accepting new calls

Esta conexión no está aceptando nuevas llamadas (conexiones). Sin embargo, las conexiones que ya estén en ejecución en el circuito virtual se mantendrán activadas.

La información mostrada para la conexión está formada por las señales de conexión local y remota y el estado actual. Para los protocolos IP (es decir, UDP+ y TCP/IP), también se mostrarán las direcciones IP local y de destino asociadas con la conexión, si se conocen.

Mandatos de supervisión de interfaces de canal (Talk 5)

Local Connection Token

La señal del dispositivo que representa esta conexión.

Remote Connection Token

La señal del sistema principal que representa esta conexión. Este campo está en blanco si no se conoce.

States for the Connection

Los estados para la conexión son:

Reset La conexión está inactiva actualmente

Pending Active - callee

Esta parte está a punto de responder a la petición de llamada de la otra parte.

Pending Active - caller

Esta parte ha llamado a la otra parte y está esperando que la otra parte responda a la llamada.

Pending Active - awaiting datastart

La conexión espera que ambas partes estén preparadas para permitir que fluyan los datos de usuario.

Active Activo y utilizable

Local IP address

La dirección IP de la interfaz MPC+ del dispositivo que está asociado con esta conexión. Este campo sólo se visualizará para los protocolos IP.

Destination IP Address

La dirección IP del sistema principal que está asociado a esta conexión. Este campo sólo se visualizará para los protocolos IP.

Ejemplo: Lista de conexiones activas para MPC+

```
MPC+>1i conn
MPC+ Connections
Virtual Circuit Token = 090144C22C00000000D
Remote Registration Token(s) = 05000101A5
Protocol = APPN, State = Active-both sides
                Local Connection Token = 090144C33000000000E
                Remote Connection Token = 05000101A6
                State = Active

Protocol = TCP/IP, State = Active-both sides
                Local Connection Token = 090144C44000000000F
                Remote Connection Token = 05000101B0
                State = Active
                Local IP address = 100.0.0.1
                Destination IP address = 100.0.0.2
```

Ejemplo: Lista de ninguna conexión activa para MPC+

```
MPC+>1i conn
No User Connections on this MPC+ Group
```

mpc

Visualiza información acerca del Grupo MPC+. Visualiza la señal de registro local y remoto, si se conoce, y el estado actual del Grupo MPC+. Si MPC+ es para uso exclusivo de UDP+, también se indicará. Si el Grupo MPC+ no es para uso exclusivo de UDP+, no se mencionará el uso exclusivo en la pantalla.

Nota: UDP+ no está soportado en un Adaptador de Canal Paralelo (PCA).

Ejemplo:

Mandatos de supervisión de interfaces de canal (Talk 5)

```
MPC+>1i mpc
MPC+ Group
Tuning Information: ACKLEN= 10, BLKTIMER= 5
Local registration token = 0901422A3C00000000
Remote registration token = 050001019D
state = Active
This MPC+ Group is for the exclusive use of UDP+.
Outbound protocol data blocking is enabled for the MPC+ Group.
```

Acklen

El tamaño (en bytes) de las tramas de reconocimiento en esta interfaz de red.

Blktimer

El tiempo máximo (en milisegundos) que se ha de esperar antes de enviar un bloque de datos incompleto al sistema principal.

Local registration token

Señal del dispositivo que representa este Grupo MPC+.

Remote registration token

Señal del sistema principal que representa este Grupo MPC+. Este campo está en blanco si no se conoce.

State El estado del Grupo MPC+:

Reset El Grupo MPC+ está inactivo actualmente.

Pending Active-xid2(00)

En el proceso de activarse y procesando xid2(00)s actualmente.

Pending Active-xid2(07)

En el proceso de activarse y procesando xid2(07)s actualmente.

Active Activo y utilizable.

Pending Reset

Pendiente de inactividad (es decir, desactivándose).

subchannel

Muestra información acerca de los subcanales que forman parte del Grupo MPC+. Muestra el número de subcanal local, el número de partición lógica, la Dirección de enlace, la dirección lógica de la Unidad de control (CU), la Dirección del dispositivo, el tipo de Subcanal (READ o WRITE) y el estado actual del subcanal. El tipo debe ser opuesto al que está configurado en el sistema principal.

Ejemplo: Lista de subcanales para MPC+

```
MPC+>1i sub
MPC+ Subchannels
Local  Link  CU Log.  Device
number LPAR  addr  address  address  type  state
-----
      1   0   F4     0     9     READ  Active
      0   0   F4     0     8     WRITE Active
```

Nota: Sólo se visualiza la dirección del dispositivo cuando se lista un subcanal PCA.

Local number

El índice de direcciones de subcanal utilizado internamente por el dispositivo.

Mandatos de supervisión de interfaces de canal (Talk 5)

Nota: La Dirección lógica CU, la Dirección de enlace y el LPAR sólo se visualizan para adaptadores ESCON.

LPAR Número de partición lógica. Permite que múltiples particiones de un sistema principal particionado lógicamente (LPAR) compartan una fibra ESCON.

Este valor se define en el Programa de configuración de la entrada/salida (IOCP) por la macroinstrucción RESOURCE.

Si el sistema principal no utiliza EMIF, el número de LPAR es 0 (cero).

Link Address

Si hay un Director ESCON (ESCD) en la vía de acceso de comunicación, la dirección del enlace es el número de puerto ESCD que está conectado al sistema principal.

Si hay dos ESCD en la misma vía de acceso, la dirección del enlace es el número de puerto de la parte del sistema principal del ESCD definido con la conexión dinámica.

Cuando no hay ningún ESCD en la vía de acceso de comunicación, este valor debe establecerse en 0x01.

CU Logical Address

La dirección de Unidad de control definida en el sistema principal para el dispositivo. Este valor se define en el Programa de configuración de la entrada/salida (IOCP) por la sentencia CUADD en la macroinstrucción CNTLUNIT.

La Dirección de unidad de control debe ser exclusiva para cada partición lógica definida en el mismo sistema principal.

Device Address

La dirección de unidad transmitida en la vía de acceso del canal para seleccionar un dispositivo. También se hace referencia como número de subcanal en la arquitectura de E/S S/370. Es un valor hexadecimal de dos dígitos en el rango de X'00' a X'FF'. Este valor se define en el IOCP del sistema principal por la sentencia UNITADD en la macroinstrucción CNTLUNIT para el dispositivo real. Es un valor hexadecimal de dos dígitos en el rango de X'00' a X'FF'. Este valor se define en el IOCP del sistema principal por la sentencia UNITADD en la macroinstrucción CNTLUNIT para el dispositivo real.

Type Si se trata de un subcanal de lectura o de grabación.

state El estado del subcanal:

Reset El subcanal está inactivo actualmente.

Pending Active-xid2(00)

El subcanal se está activando y está procesando xid2(00)s actualmente.

Pending Active-xid2(07)

El subcanal se está activando y actualmente está procesando xid2(07)s.

Active El subcanal está activo y forma parte de un Grupo MPC+.

Mandatos de supervisión de interfaces de canal (Talk 5)

Pending Reset

El subcanal está pendiente de inactividad (es decir se está desactivando).

Tune

Utilice el mandato **tune** para modificar varios parámetros de manejador de red MPC+.

Sintaxis:

tune acklen
blktimer

acklen

El tamaño (en bytes) de las tramas de reconocimiento de esta interfaz de red MPC+.

Valores válidos: De 0 a 500

Valores por omisión: Se solicitará el valor de entrada

Nota: El manejador de red base con el cual está asociado el manejador de red MPC+ debe estar activado para que se pueda modificar este campo.

blktimer

El tiempo máximo (en milisegundos) que se ha de esperar antes de enviar un bloque de datos incompleto al sistema principal.

Valores válidos: De 0 a 20

Valores por omisión: Se solicitará el valor de entrada

Nota: El manejador de red base con el cual está asociado el manejador de red MPC+ debe estar activado para que se pueda modificar este campo.

Capítulo 30. Soporte para la reconfiguración dinámica del canal ESCON

Esta sección describe la reconfiguración dinámica (DR) en la medida en que afecta a los mandatos Talk 6 y Talk 5.

Delete Interface de CONFIG (Talk 6)

El canal ESCON soporta el mandato **delete interface** de CONFIG (Talk 6) con las consideraciones siguientes:

- También se suprimirán todas las interfaces virtuales (LSA, LCS, MPC) de esta interfaz ESCON.
- Si se trata de la última interfaz de canal (ESCON o PCA) de la máquina, también se suprimirá la interfaz de bucle de retorno APPN si existe.

Activate Interface de GWCON (Talk 5)

El canal ESCON soporta el mandato **activate interface** de GWCON (Talk 5) con la consideración siguiente:

El tamaño de MAXDATA no se establecerá en un valor superior al tamaño del almacenamiento intermedio asignado por el direccionador en el rearranque.

El mandato **activate interface** de GWCON (Talk 5) soporta todos los mandatos específicos de interfaz del canal ESCON.

Reset Interface de GWCON (Talk 5)

El canal ESCON soporta el mandato **reset interface** de GWCON (Talk 5) con las consideraciones siguientes:

- También se restablecerán todas las interfaces virtuales (LSA, LCS, MPC) de esta interfaz ESCON.
- Todas las interfaces virtuales (LSA, LCS, MPC) deben permitir el restablecimiento de su interfaz. Las razones por las que una red virtual no permitiría el restablecimiento de su red base son: Para MPC, si la nueva configuración tiene más subcanales que la configuración que está activa actualmente y MPC no puede obtener almacenamiento adicional para soportar estos subcanales nuevos, no se realizará el restablecimiento. Si se necesita almacenamiento adicional, se visualizará un mensaje en la consola.
- El tamaño de MAXDATA no se establecerá en un valor superior al tamaño del almacenamiento intermedio asignado por el direccionador en el rearranque.

El mandato **reset interface** de GWCON (Talk 5) soporta todos los mandatos específicos de interfaz del canal ESCON.

Mandatos de cambio temporal de GWCON (Talk 5)

El canal ESCON soporta los mandatos GWCON siguientes que cambian temporalmente el estado operativo del dispositivo. Estos cambios se pierden cuando se vuelve a cargar o se reinicia el dispositivo o cuando se ejecuta algún mandato reconfigurable dinámicamente.

Mandatos

GWCON, net, tune iplow Nota: Permite modificar la señal de mínimo para la agrupación de almacenamientos intermedios privados utilizada para la última entrada de vía rápida.
GWCON, net, tune opfair Nota: Permite modificar el número “fair” (razonable) de paquetes que esta interfaz puede poner en cola.
GWCON, net, trace Nota: Permite activar y desactivar la modalidad de rastreo para el microcódigo del adaptador ESCON.

Capítulo 31. Soporte para la reconfiguración dinámica del canal PCA

Esta sección describe la reconfiguración dinámica (DR) en la medida en que afecta a los mandatos Talk 6 y Talk 5.

Delete Interface de CONFIG (Talk 6)

El canal PCA soporta el mandato **delete interface** de CONFIG (Talk 6) con las consideraciones siguientes:

- También se suprimirán todas las interfaces virtuales (LSA, LCS, MPC) de esta interfaz PCA.
- Si se trata de la última interfaz de canal (ESCON o PCA) de la máquina, también se suprimirá la interfaz de bucle de retorno APPN si existe.

Activate Interface de GWCON (Talk 5)

El canal PCA soporta el mandato **activate interface** de GWCON (Talk 5) con la consideración siguiente:

El tamaño de MAXDATA no se establecerá en un valor superior al tamaño del almacenamiento intermedio asignado por el direccionador en el rearranque.

El mandato **activate interface** de GWCON (Talk 5) soporta todos los mandatos específicos de interfaz del canal PCA.

Reset Interface de GWCON (Talk 5)

El canal PCA soporta el mandato **reset interface** de GWCON (Talk 5) con las consideraciones siguientes:

- También se restablecerán todas las interfaces virtuales (LSA, LCS, MPC) de esta interfaz PCA.
- Todas las interfaces virtuales (LSA, LCS, MPC) deben permitir el restablecimiento de su interfaz. Una razón por la que una red virtual no permitiría el restablecimiento de su red base sería:

Para MPC, si la nueva configuración tiene más subcanales que la configuración que está activa actualmente y MPC no puede obtener almacenamiento adicional para soportar estos subcanales nuevos, no se realizará el restablecimiento. Si se necesita almacenamiento adicional, se visualizará un mensaje en la consola.

- El tamaño de MAXDATA no se establecerá en un valor superior al tamaño del almacenamiento intermedio asignado por el direccionador en el rearranque.

El mandato **reset interface** de GWCON (Talk 5) soporta todos los mandatos específicos de interfaz del canal PCA.

Mandatos de cambio temporal de GWCON (Talk 5)

El canal PCA soporta los mandatos GWCON siguientes que cambian temporalmente el estado operativo del dispositivo. Estos cambios se pierden cuando se vuelve a cargar o se reinicia el dispositivo o cuando se ejecuta algún mandato reconfigurable dinámicamente.

Mandatos

GWCON, net, tune iplow Nota: Permite modificar la señal de mínimo para la agrupación de almacenamientos intermedios privados utilizada para la última entrada de vía rápida.
GWCON, net, tune opfair Nota: Permite modificar el número "fair" (razonable) de paquetes que esta interfaz puede poner en cola.
GWCON, net, trace Nota: Permite activar y desactivar la modalidad de rastreo para el microcódigo del adaptador PCA.
GWCON, net, hidtrace Nota: Permite activar y desactivar el rastreo HID para el adaptador PCA.

Capítulo 32. Soporte para la reconfiguración dinámica del canal virtual LSA

Esta sección describe la reconfiguración dinámica (DR) en la medida en que afecta a los mandatos Talk 6 y Talk 5.

Delete Interface de CONFIG (Talk 6)

El canal virtual LSA soporta el mandato **delete interface** de CONFIG (Talk 6) sin ninguna restricción.

Activate Interface de GWCON (Talk 5)

El canal virtual LSA soporta el mandato **activate interface** de GWCON (Talk 5) con las consideraciones siguientes:

- La interfaz del canal base (ESCON o PCA) para esta interfaz virtual LSA debe estar activa.
- MAXDATA para esta interfaz virtual LSA no puede ser superior al MAXDATA mayor de las interfaces virtuales que ya están en la interfaz del canal base (ESCON o PCA) en la que está esta interfaz virtual LSA.
- Los subcanales de esta interfaz LSA no pueden estar utilizándose por otra interfaz virtual no LSA (MPC o LCS) de la interfaz del canal base (ESCON o PCA) en la que está esta interfaz virtual LSA.
- La adición de subcanales nuevos a la interfaz del canal base (ESCON o PCA) no hará que ésta sobrepase su número máximo de canales.
- Hay suficiente almacenamiento para añadir otra interfaz virtual a la interfaz del canal base (ESCON o PCA). Si se necesita almacenamiento adicional, se visualizará un mensaje en la consola.

El mandato **activate interface** de GWCON (Talk 5) soporta todos los mandatos específicos de interfaz del canal virtual LSA.

Reset Interface de GWCON (Talk 5)

El canal virtual LSA soporta el mandato **reset interface** de GWCON (Talk 5) con las consideraciones siguientes:

- No se permitirá el restablecimiento de la interfaz virtual LSA si para los cambios es necesario modificar el adaptador. Es necesario modificar el adaptador si:
 1. Se ha cambiado el tipo de LAN o el número de LAN.
 2. Se ha cambiado BLKLEN o ACKLEN.
 3. Se han cambiado los subcanales, se ha añadido un subcanal nuevo o se ha suprimido un subcanal existente de la interfaz LSA. Para cambiar cualquiera de los elementos anteriores, debe restablecerse toda la interfaz del canal base (ESCON o PCA).
- La interfaz virtual LSA ya debe estar activa.
- MAXDATA para la interfaz virtual LSA no debe ser superior al MAXDATA mayor de la interfaz del canal base (ESCON o PCA).

El mandato **reset interface** de GWCON (Talk 5) soporta todos los mandatos específicos de interfaz del canal virtual LSA.

Mandatos de cambio temporal de GWCON (Talk 5)

El canal virtual LSA soporta los mandatos GWCON siguientes que cambian temporalmente el estado operativo del dispositivo. Estos cambios se pierden cuando se vuelve a cargar o se reinicia el dispositivo o cuando se ejecuta algún mandato reconfigurable dinámicamente.

Mandatos
GWCON, net, tune acklen Nota: Cambia el valor operativo de ACKLEN (longitud de reconocimiento)
GWCON, net, tune blktimer Nota: Cambia el valor operativo de BLKTIMER (temporizador de bloqueos)

Capítulo 33. Soporte para la reconfiguración dinámica del canal virtual LCS

Esta sección describe la reconfiguración dinámica (DR) en la medida en que afecta a los mandatos Talk 6 y Talk 5.

Delete Interface de CONFIG (Talk 6)

El canal virtual LCS soporta el mandato **delete interface** de CONFIG (Talk 6) sin ninguna restricción.

Activate Interface de GWCON (Talk 5)

El canal virtual LCS soporta el mandato **activate interface** de GWCON (Talk 5) con las consideraciones siguientes:

- La interfaz del canal base (ESCON o PCA) para esta interfaz virtual LCS debe estar activa.
- MAXDATA para esta interfaz virtual LCS no puede ser superior al MAXDATA mayor de las interfaces virtuales que ya están en la interfaz del canal base (ESCON o PCA) en la que está esta interfaz virtual LCS.
- Los subcanales de esta interfaz virtual LCS no pueden estar utilizándose por otra interfaz virtual no LCS (MPC o LSA) de la interfaz del canal base (ESCON o PCA) en la que está esta interfaz virtual LCS.
- La adición de subcanales nuevos a la interfaz del canal base (ESCON o PCA) no hará que ésta sobrepase su número máximo de canales.
- Hay suficiente almacenamiento para añadir otra interfaz virtual a la interfaz del canal base (ESCON o PCA). Si se necesita almacenamiento adicional, se visualizará un mensaje en la consola.

El mandato **activate interface** de GWCON (Talk 5) soporta todos los mandatos específicos de interfaz del canal virtual LCS.

Reset Interface de GWCON (Talk 5)

El canal virtual LCS soporta el mandato **reset interface** de GWCON (Talk 5) con las consideraciones siguientes:

- No se permitirá el restablecimiento de la interfaz virtual LCS si para los cambios es necesario modificar el adaptador. Es necesario modificar el adaptador si:
 1. Se ha cambiado el tipo de LAN o el número de LAN
 2. Se ha cambiado BLKLEN o ACKLEN
 3. Se han cambiado los subcanales para esta interfaz LCS. Para cambiar cualquiera de los elementos anteriores, debe restablecerse toda la interfaz del canal base (ESCON o PCA).
- La interfaz virtual LCS ya debe estar activa.
- MAXDATA para la interfaz virtual LCS no debe ser superior al MAXDATA mayor de la interfaz del canal base (ESCON o PCA).

El mandato **reset interface** de GWCON (Talk 5) soporta todos los mandatos específicos de interfaz del canal virtual LCS.

Mandatos de cambio temporal de GWCON (Talk 5)

El canal virtual LCS soporta los mandatos GWCON siguientes que cambian temporalmente el estado operativo del dispositivo. Estos cambios se pierden cuando se vuelve a cargar o se reinicia el dispositivo o cuando se ejecuta algún mandato reconfigurable dinámicamente.

Mandatos
GWCON, net, tune acklen Nota: Cambia el valor operativo de ACKLEN (longitud de reconocimiento)
GWCON, net, tune blktimer Nota: Cambia el valor operativo de BLKTIMER (temporizador de bloqueos)

Capítulo 34. Soporte para la reconfiguración dinámica del canal virtual MPC

Esta sección describe la reconfiguración dinámica (DR) en la medida en que afecta a los mandatos Talk 6 y Talk 5.

Delete Interface de CONFIG (Talk 6)

El canal virtual MPC soporta el mandato **delete interface** de CONFIG (Talk 6) sin ninguna restricción.

Activate Interface de GWCON (Talk 5)

El canal virtual MPC soporta el mandato **activate interface** de GWCON (Talk 5) con las consideraciones siguientes:

- La interfaz del canal base (ESCON o PCA) para esta interfaz virtual MPC debe estar activa.
- MAXDATA para esta interfaz virtual MPC no puede ser superior al MAXDATA mayor de las interfaces virtuales que ya están en la interfaz del canal base (ESCON o PCA) en la que está esta interfaz virtual MPC.
- Los subcanales de esta interfaz virtual MPC no pueden estar utilizándose por otra interfaz virtual no (MPC, LCS o LSA) de la interfaz del canal base (ESCON o PCA) en la que está esta interfaz virtual MPC.
- La adición de subcanales nuevos a la interfaz del canal base (ESCON o PCA) no hará que ésta sobrepase su número máximo de canales.
- Hay suficiente almacenamiento para añadir otra interfaz virtual a la interfaz del canal base (ESCON o PCA). Si se necesita almacenamiento adicional, se visualizará un mensaje en la consola.

El mandato **activate interface** de GWCON (Talk 5) soporta todos los mandatos específicos de interfaz del canal virtual MPC.

Reset Interface de GWCON (Talk 5)

El canal virtual MPC soporta el mandato **reset interface** de GWCON (Talk 5) con las consideraciones siguientes:

- No se permitirá el restablecimiento de la interfaz virtual MPC si para los cambios es necesario modificar el adaptador. Es necesario modificar el adaptador para los cambios siguientes:
 - Cambiar el tipo de LAN o el número de LAN.
 - Cambiar BLKLEN o ACKLEN.
 - Cambiar los subcanales, añadir un subcanal nuevo o suprimir un subcanal existente de esta interfaz MPC.

Para realizar cualquiera de estos cambios, es necesario restablecer toda la interfaz del canal base (ESCON o PCA).

- La interfaz virtual MPC ya debe estar activa.
- MAXDATA para la interfaz virtual MPC no debe ser superior al MAXDATA mayor de la interfaz del canal base (ESCON o PCA).

El mandato **reset interface** de GWCON (Talk 5) soporta todos los mandatos específicos de interfaz del canal virtual MPC.

Mandatos de cambio temporal de GWCON (Talk 5)

El canal virtual MPC soporta los mandatos GWCON siguientes que cambian temporalmente el estado operativo del dispositivo. Estos cambios se pierden cuando se vuelve a cargar o se reinicia el dispositivo o cuando se ejecuta algún mandato reconfigurable dinámicamente.

Mandatos
GWCON, net, tune acklen Nota: Cambia el valor operativo de ACKLEN (longitud de reconocimiento)
GWCON, net, tune blktimer Nota: Cambia el valor operativo de BLKTIMER (temporizador de bloqueos)

Capítulo 35. Soporte para la reconfiguración dinámica de la interfaz de bucle de retorno APPN

Esta sección describe la reconfiguración dinámica (DR) en la medida en que afecta a los mandatos Talk 6 y Talk 5.

Delete Interface de CONFIG (Talk 6)

La interfaz de bucle de retorno APPN soporta el mandato **delete interface** de CONFIG (Talk 6) sin ninguna restricción.

Activate Interface de GWCON (Talk 5)

La interfaz de bucle de retorno APPN soporta el mandato **activate interface** de GWCON (Talk 5) sin ninguna restricción.

El mandato **activate interface** de GWCON (Talk 5) soporta todos los mandatos específicos de interfaz de bucle de retorno APPN.

Reset Interface de GWCON (Talk 5)

La interfaz de bucle de retorno APPN soporta el mandato **reset interface** de GWCON (Talk 5) sin ninguna restricción.

El mandato **reset interface** de GWCON (Talk 5) soporta todos los mandatos específicos de interfaz de bucle de retorno APPN.

Capítulo 36. Configuración de interfaces de línea serie

Este capítulo describe el proceso de configuración de interfaces para una interfaz serie e incluye las secciones siguientes:

- “Acceso al proceso de configuración de interfaces”
- “Interfaces de red y el mandato interface de GWCON” en la página 460

IMPORTANTE: Para configurar los protocolos Frame Relay, PPP, X.25, V.25bis, SDLC Relay y SDLC en la interfaz serie, utilice los mandatos de este capítulo y después consulte los mandatos de los capítulos que describen el protocolo específico.

Consulte la sección “Configuración de la interfaz de red” en la página 19 para ver una tabla de protocolos y las interfaces que dan soporte a estos protocolos.

Acceso al proceso de configuración de interfaces

Consulte la sección “Adición de dispositivos” en la página 16 para ver una descripción de cómo añadir una interfaz serie. Una vez haya hecho esto, los párrafos siguientes describen cómo establecer el enlace de datos de la interfaz correctamente y cómo acceder a los mandatos de configuración de ese enlace de datos.

Para acceder al proceso de configuración de interfaces para una interfaz serie, primero acceda al indicador `Config>` y emita el mandato **set data-link**. Después, en el indicador `Config>`, entre el tipo y número de interfaz para acceder al entorno de configuración para la interfaz.

Por ejemplo, para configurar una interfaz serie para X.25, debe acceder al entorno `X.25 config>` emitiendo los mandatos siguientes:

```
Config> set data-link X25 2
Config> network 2
```

En el entorno `X.25 config>`, puede completar la configuración de X.25 de la interfaz serie. Consulte la sección “Capítulo 37. Utilización de la interfaz de red X.25” en la página 461.

Cuando haya terminado de configurar la interfaz serie, entre el mandato **restart** después del indicador `OPCON (*)` y responda **yes** a la solicitud de habilitar la nueva configuración.

Cronometraje y tipo de cable

Esta sección se aplica a todos los usuarios de un puerto serie para: FR, PPP, X.25, SDLC Relay y SDLC.

Si se conecta un módem o CSU/DSU al puerto serie, el direccionador cumple la función del DTE en lo referente al cronometraje de la línea, por lo tanto configure un tipo de cable DTE y un cronometraje externo.

Si desea conectar dos direccionadores directamente sin ningún módem, CSU/DSU ni eliminador de módem, entonces uno de los direccionadores cumplirá la función del DCE en lo referente al cronometraje de la línea. Conecte un cable de conexión directa al direccionador que va a actuar como DCE y configure los parámetros siguientes para su interfaz serie.

Configuración de interfaces de línea serie

1. Un tipo de cable DCE
2. Cronometraje interno
3. El cronometraje/velocidad de línea

El otro direccionador cumplirá la función de DTE en lo referente al cronometraje y debe configurarse como si estuviese conectado a un módem o CSU/DSU.

Nota: La configuración de un DTE y no un cable DCE no influye en si el manejador de red WAN cumple la función del dispositivo similar o no. Por ejemplo, el direccionador actúa siempre como un dispositivo DTE Frame Relay y utiliza una interfaz FR UNI incluso cuando hay una interfaz Frame Relay configurada para utilizar un cable DCE.

Interfaces de red y el mandato interface de GWCON

Aunque las interfaces de línea serie no tienen su propio proceso de consola para la supervisión, los direccionadores pueden visualizar estadísticas completas para todas las interfaces de red instaladas cuando se utiliza el mandato **interface** en el entorno GWCON. Para obtener más información sobre el mandato **interface** y la visualización de estadísticas, consulte la sección Capítulo 8. El proceso de operación/supervisión (GWCON - Talk 5) y sus mandatos.

Capítulo 37. Utilización de la interfaz de red X.25

La interfaz de red X.25 conecta un direccionador a una red conmutada de circuito virtual X.25. El software y el hardware de la interfaz de red X.25 permiten que el direccionador se comunique a través de una red X.25 pública. La interfaz de red X.25 cumple con las especificaciones CCITT 1980, CCITT 1984, CCITT 1988 e ISO 8208 1990 para interfaces X.25 que ofrecen canales multiplexados y transferencia de datos fiable de extremo a extremo en una red de área amplia.

Este capítulo incluye las secciones siguientes:

- “Procedimientos de configuración básica”
- “Encapsulación nula” en la página 464
- “Comprensión de los grupos de usuarios cerrados” en la página 465

Para obtener información sobre la configuración de X.25 Transport Protocol (XTP) para transportar tráfico X.25 a través de TCP/IP, consulte la sección “Capítulo 39. Utilización de XTP” en la página 505.

Procedimientos de configuración básica

Esta sección indica los pasos de configuración mínima necesarios para que la interfaz X.25 se active y ejecute. Los parámetros de X.25 deben ser coherentes con la red X.25 con la que se conectará la interfaz del direccionador. Para obtener más información, consulte los mandatos de configuración descritos en este capítulo.

Nota: Debe reiniciar el direccionador para que los cambios en la configuración surtan efecto.

1. En el indicador OPCON (*), escriba **talk 6**.
Aparece el indicador `Config>`.
2. Escriba **list devices** para visualizar una lista de interfaces entre las que puede seleccionar. Utilice el número de interfaz adecuado en el paso siguiente.
3. Escriba **set data-link x25**.
Aparece el indicador `Interface Number [0]?`.
4. Escriba el número de interfaz adecuado.
5. Conéctese a la red escribiendo **net número** en el indicador `Config>`.
Aparece el indicador `X.25 Config [número]>`.
6. En este indicador, escriba **set address dirección-nodo-x.25**.
La dirección X.25 es una dirección X.121 exclusiva que se utiliza durante el establecimiento de llamadas. Para redes DDN, utilice los mandatos **add htf-addr** y **set htf-addr** para convertir la dirección de protocolo asociada con esta interfaz en el formato de dirección X.121 necesario para la conversión de direcciones DDN. La imposibilidad de establecer la dirección de la red impide que la interfaz X.25 se una a la red conectada.
7. Escriba **set equipment-type** y especifique si los niveles de trama y de paquete actúan como DCE o DTE. El valor por omisión para este mandato es DTE.
8. Escriba **set svc** y defina los SVC inferior y superior que está utilizando. El valor por omisión es para 1 SVC.
9. Escriba **add protocol nombre_protocolo** para añadir los protocolos que se ejecutarán en la interfaz X.25. Se solicitará el tamaño de ventana, el tamaño

Utilización de la interfaz de red X.25

de paquete por omisión, el tamaño máximo de paquete, el tiempo de desocupado del circuito y el VC máximo.

Nota: Sólo es necesario añadir los protocolos una vez para todas las redes X.25 del direccionador.

10. Escriba **add address nombre_protocolo** para añadir una conversión de dirección para la dirección de destino de cada protocolo al que se puede llegar a través de esta interfaz.
11. Escriba **exit** para volver al indicador Config>.
12. Pulse **Control-P** para volver al indicador OPCON (*).
13. Escriba **restart** y responda **yes** a la solicitud.

Establecimiento de la personalidad nacional

Cada red de datos pública como, por ejemplo Telenet de GTE o Defense Data Network de DDN, tiene su propia configuración estándar. El término *Personalidad nacional* especifica un grupo de variables utilizadas para definir las características de una red de datos pública. La información de configuración de la Personalidad nacional proporciona al direccionador información de control para los paquetes que se transfieren en el enlace. La opción de Personalidad nacional define 27 parámetros por omisión para cada red de datos pública.

Para ver los valores de configuración que están en la Personalidad nacional X.25, ejecute el mandato de configuración X.25 **list detailed**. Configure cada red de datos pública conectada al direccionador ejecutando el mandato de configuración **national-personality set** de X.25.

La Personalidad nacional es un modelo generalizado para la configuración de la red. Si es necesario, puede configurar individualmente cada parámetro de capa de trama y de paquete.

Comprensión de los valores por omisión de X.25

Las tablas siguientes listan los valores por omisión de los diversos parámetros para los mandatos X.25 *set*, *national set* y *national enable*.

Tabla 57. Mandato set

Parámetro	Valor por omisión
<u>address</u> ...	ninguno
<u>cable</u>	ninguno
<u>calls-out</u> ...	4
<u>clocking</u> ...	external
<u>default-window-size</u> ...	2
<u>encoding</u>	NRZ
<u>equipment-type</u> ...	DTE
<u>htf addr</u> ...	ninguno
<u>inter-frame-delay</u> ...	0
<u>mtu</u>	1500
<u>national-personality</u> ...	GTE Telenet
<u>pvc</u> ...	low=0 high=0
<u>speed</u>	9600

Utilización de la interfaz de red X.25

Tabla 57. Mandato set (continuación)

Parámetro	Valor por omisión
svc	low inbound=0, high inbound=0 low 2-way=1, high 2-way=64 low outbound=0, high outbound=0
throughput-class ...	inbound=outbound=2400
vc-idle ...	30

Tabla 58. Parámetros de National Enable

Parámetro	Valor por omisión de DDN	Valor por omisión de GTE
accept-reverse-charges	off	on
bi-cug	off	off
bi-cug-with-outgoing-access	off	off
cug	off	off
cug-deletion	off	off
cug-insertion	off	off
cug-with-incoming-access	off	off
cug-with-outgoing-access	off	off
cug-zero-override	off	off
flow-control-negotiation	on	on
frame-ext-seq-mode	off	off
packet-ext-seq-mode	off	off
request-reverse-charges	off	on
suppress-calling-addresses	off	off
throughput-class-negotiation	on	on
truncate-called-addresses	off	off

Tabla 59. Parámetros de National Set

Parámetro	Valor por omisión de DDN	Valor por omisión de GTE
call-req	20 decasegundos	20 decasegundos
clear-req ...	reintentos=1	reintentos=1
	18 decasegundos	18 decasegundos
disconnect-procedure ...	pasivo	pasivo
dly-recall-timer...	0	0
dp-timer	500 milisegundos	500 milisegundos
frame-window-size	7	7
n2-timeouts	20	20
packet-size ...	128, máx=256	128, máx=256
reset ...	reintentos=1	reintentos=1
	18 decasegundos	18 decasegundos

Utilización de la interfaz de red X.25

Tabla 59. Parámetros de National Set (continuación)

Parámetro	Valor por omisión de DDN	Valor por omisión de GTE
<u>restart</u> ...	reintentos=1 18 decasegundos	reintentos=1 18 decasegundos
<u>max-recall-retires</u> ...	3	3
<u>min-recall</u>	10 segundos	10 segundos
<u>min-connect</u>	90 segundos	90 segundos
<u>collision-timer</u>	10 segundos	10 segundos
<u>standard-version</u>	1984	1984
<u>t1-timer</u>	4 segundos	4 segundos
<u>t2-timer</u>	0	0
<u>truncate-called-addr-size</u>	2	2

Encapsulación nula

La Encapsulación nula permite al usuario multiplexar varios protocolos de capa de red a través de un circuito X.25. Esta función puede utilizarse para evitar utilizar un número no razonable de circuitos virtuales.

Límites

La Encapsulación nula no está soportada para QLLC. Esta función se soporta para Circuitos virtuales conmutadas (SVC), pero no para los Circuitos virtuales permanentes (PVC).

Cambios de configuración

Se ha añadido la opción de encapsulación NULL para los mandatos T6 siguientes:

- Bajo X25 config: add address IP (puede entrar el tipo de enc. = NULL)
- Bajo X25 config: add address IPX (puede entrar el tipo de enc. = NULL)
- Bajo X25 config: add address DNA (puede entrar el tipo de enc. = NULL)
- Bajo X25 config: add address VINES (puede entrar el tipo de enc. = NULL)
- Bajo X25 config: list addr mostrará el tipo de enc. activo = NULL si el tipo de prioridad 1 es NULL.

Mandatos T5:

- Bajo X25 int: List SVCS incluirá el tipo de enc. = NULL

Configuración de encapsulación nula y Grupos de usuarios cerrados (CUG)

Ya que pueden ejecutarse más de un protocolo a través de un circuito virtual cuando se utiliza la Encapsulación nula, los CUG definidos para cada protocolo a través de este circuito debe ser los mismos. Se sugiere encarecidamente que el usuario configure múltiples protocolos con el mismo destino tal como sigue:

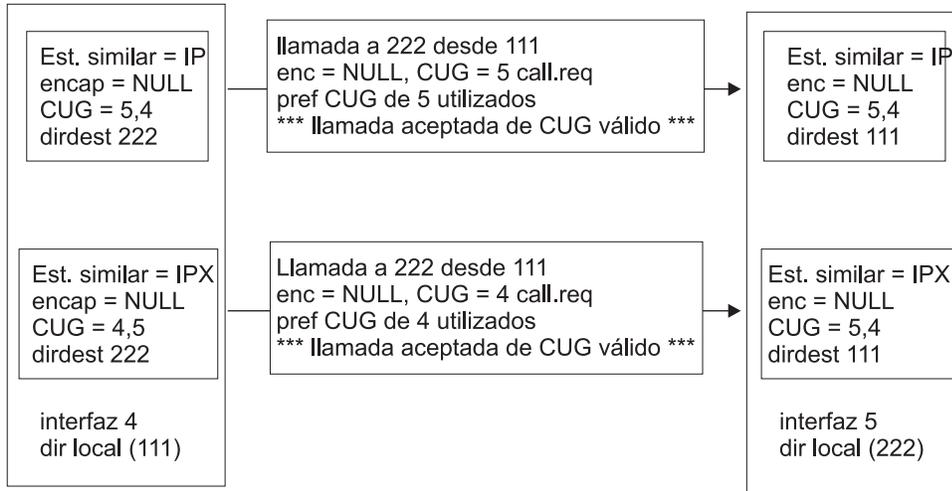
Configure el CUG utilizando add address. Los CUG definidos deben ser los mismos para cada protocolo definido en la misma dirección.

Si el CUG se define en el nivel de add protocol, los CUG deben ser los mismos para todos los similares. (Este método es más restrictivo).

Configure CUG a nivel de interfaz. Esto asegura que todos los similares tienen los mismos valores de CUG. (Este método es el más restrictivo)

Cualquiera de los métodos anteriores puede utilizarse siempre que alguna definición de CUG de llamada interno sea válida para todos los protocolos que comparten este circuito. Válido significa que el CUG se haya definido para la dirección específica o haya tomado por omisión utilizar la definición de protocolo o de circuito de interfaz.

CASO 1: Grupos cerrados de usuarios (CUG) de entrada válidos para ambas estaciones similares.



CASO 2: Grupos cerrados de usuarios (CUG) de entrada no válidos para ambas estaciones similares.

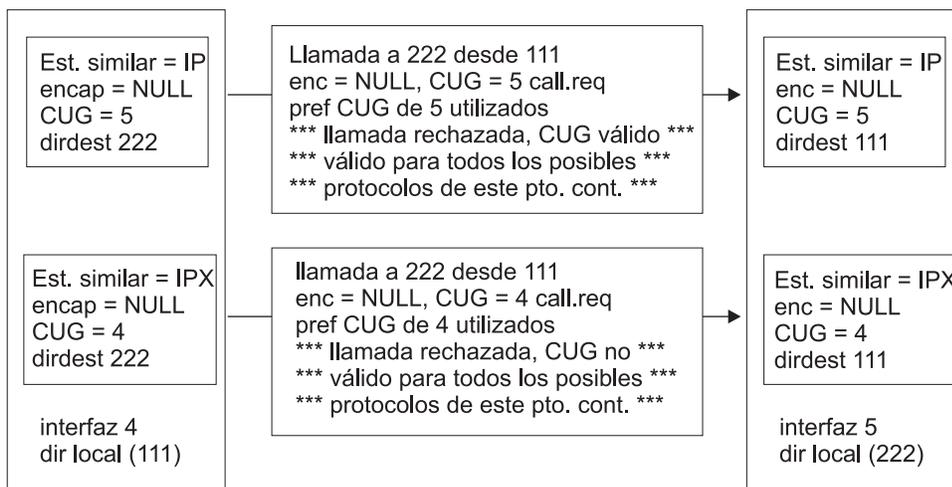


Figura 35. Encapsulación nula de grupo de usuarios cerrado

Comprensión de los grupos de usuarios cerrados

Un grupo de usuarios cerrado (CUG) es un grupo de DTE X.25 que tiene permitido establecer conexiones con otros DTE específicos. Los números de CUG los define el proveedor de la red y sólo puede utilizar los CUG que el proveedor le asigne. Puede configurar un CUG específico de dirección, un CUG específico de protocolo

Utilización de la interfaz de red X.25

o un CUG específico de interfaz. Si se configuran los tres tipos de números de CUG para un DTE, el recurso de grupo de usuarios cerrado utiliza el CUG de destino específico de dirección en una petición de llamada al ponerse en contacto con otro DTE. Si sólo se configura un CUG específico de protocolo y otro específico de interfaz para un DTE, el recurso de grupo de usuarios cerrado utiliza el CUG específico de protocolo en una llamada de petición al establecer contacto con otro DTE.

Un solo DTE puede pertenecer a múltiples CUG. Debe especificar un CUG preferido para este DTE. El CUG preferido se utiliza cuando el direccionador inicia llamadas a otros DTE. Un solo DTE no puede tener más de un total de 5 grupos de usuarios cerrados normales o preferidos.

Grupos de usuarios cerrados bilaterales

Un *grupo de usuarios cerrado bilateral (BCUG)* es un grupo de usuarios cerrado que sólo consta de dos DTE. Los DTE del BCUG pueden originar llamadas a los miembros del BCUG y a cualquier DTE que no sea miembro de cualquier CUG o BCUG. Un solo DTE no puede tener más de un total de 5 CUG bilaterales preferidos o normales.

Un DTE utiliza un BCUG para establecer circuitos de la misma manera que el DTE utiliza los CUG para establecer circuitos (consulte la Tabla 60 en la página 467), sin embargo, si se define un BCUG y un CUG para una interfaz, protocolo o dirección, se utiliza el BCUG para establecer el circuito.

Tipos de grupos de usuarios cerrados extendidos

Se da soporte a las extensiones siguientes para grupos de usuarios cerrados:

CUG con acceso externo

El DTE puede pertenecer a uno o varios CUG. El DTE puede originar llamadas a miembros del CUG y a cualquier DTE que pertenezca a otros CUG con el acceso interno.

CUG con acceso interno

El DTE puede pertenecer a uno o varios CUG. El DTE puede recibir llamadas de DTE que no pertenecen a ningún CUG o desde DTE que pertenecen a otros CUG con acceso externo.

BCUG con acceso externo

El DTE puede pertenecer a uno o varios BCUG. El DTE puede originar llamadas a miembros del BCUG y a cualquier DTE que no pertenezca a ningún BCUG.

Establecimiento de circuitos X.25 con grupos de usuarios cerrados en un dispositivo

Cuando haya habilitado el recurso de grupo de usuarios cerrado y un DTE reciba una petición de llamada, utiliza el CUG de la petición de llamada para determinar si debe aceptar o rechazar la llamada del DTE. Si el CUG de la petición de llamada no coincide con el CUG configurado en la interfaz, protocolo o destino asociado con el DTE llamador, se rechaza la petición. La Tabla 60 en la página 467 resume la forma de establecer los circuitos X.25 basándose en los CUG, si los números de CUG de interfaz, protocolo y dirección son diferentes y no está habilitado el acceso interno.

Tabla 60. Establecimiento de circuitos X.25 internos para grupos de usuarios cerrados

Contenido de la petición de llamada interna contiene	Definición de CUG de DTE receptor							
	Sólo CUG de interfaz	Sólo CUG de protocolo	CUG específico de dirección	CUG de interfaz y de protocolo	CUG de interfaz y de dirección	CUG de protocolo y dirección	Todos los CUG	Ningún CUG
Ningún CUG	Se rechaza	Se rechaza	Se rechaza	Se rechaza	Se rechaza	Se rechaza	Se rechaza	Se acepta
CUG de interfaz	Se acepta	Se rechaza	Se rechaza	Se rechaza	Se rechaza	Se rechaza	Se rechaza	Se rechaza
CUG de protocolo	Se rechaza	Se acepta	Se rechaza	Se acepta	Se rechaza	Se rechaza	Se rechaza	Se rechaza
CUG específico de dirección	Se rechaza	Se rechaza	Se acepta	Se rechaza	Se acepta	Se acepta	Se acepta	Se rechaza

Para llamadas de salida de una interfaz, si ha habilitado el recurso de CUG o de BCUG, cada petición de llamada contendrá el CUG preferido configurado (si hay alguno) para el destino o, si no se ha configurado ningún CUG específico de dirección, se utiliza el CUG definido para el protocolo o, si no se ha configurado ningún CUG específico de protocolo, se utiliza el CUG definido para la interfaz. Si no se ha configurado ningún número de CUG, el recurso de CUG no se incluye en ninguna petición de llamada de salida.

Alteración temporal del proceso del grupo de usuarios cerrado para el CUG 0

Puede configurar el DTE de manera que no valide las llamadas de entrada con un CUG de 0 en la petición de llamada. Esta posibilidad permite que se completen llamadas específicas aunque no haya habilitado el acceso interno. La utilización del mandato **national enable cug 0 override** fuerza a que el dispositivo pase por alto el recurso de CUG si el número de CUG es 0. La petición de llamada no se comparará con ningún número de CUG configurado.

Configuración de grupos de usuarios cerrados X.25

Para utilizar los grupos de usuarios cerrados en interfaces X.25:

1. Pida los números de CUG al proveedor de la red. Necesitará estos números al configurar X.25.
2. Habilite el recurso de grupo de usuarios cerrado utilizando el mandato **national enable cug** y los mandatos relacionados.
3. Habilite el recurso de grupo de usuarios cerrado bilateral, si lo desea, utilizando el mandato **national enable bi-cug** y los mandatos relacionados.
4. Configure los números de CUG adecuados para los DTE. Especifique el CUG preferido, el CUG, el CUG bilateral preferido y el CUG bilateral, según proceda. Esto se realiza mediante el mandato **add address**.
5. Configure el CUG y el CUG bilateral adecuados para el protocolo, si es necesario. Esto se realiza mediante el mandato **add protocol**.

Nota: Sólo debe configurar estos CUG si está restringiendo todos los circuitos X.25 establecidos a través de la interfaz X.25 para este protocolo a los DTE que pertenecen a este conjunto de CUG o BCUG exclusivos a menos que lo altere temporalmente con un CUG específico de dirección.

Utilización de la interfaz de red X.25

6. Configure el CUG adecuado y el CUG bilateral para la interfaz, si es necesario. Esto se realiza mediante el mandato **add cug**.

Nota: Sólo debe configurar estos CUG si limita todos los circuitos X.25 establecidos sobre la interfaz X.25 a los DTE pertenecientes a este conjunto de CUG o BCUG exclusivos, a menos que se altere temporalmente con un CUG específico de protocolo o dirección.

Capítulo 38. Configuración y supervisión de la interfaz de red X.25

Este capítulo describe los mandatos de configuración y operativos de X.25 e incluye las secciones siguientes:

- “Mandatos de configuración X.25”
- “Acceso al proceso de supervisión de interfaces” en la página 497
- “Mandatos de supervisión X.25” en la página 497
- “Interfaces de red X.25 y el mandato interface de GWCON” en la página 501
- “Soporte de la reconfiguración dinámica de la interfaz de red X.25” en la página 504

Mandatos de configuración X.25

Esta sección resume y explica todos los mandatos de configuración X.25.

Los mandatos de configuración X.25 le permiten especificar los parámetros de red para las interfaces de direccionador que transmiten paquetes X.25. La información que especifique con los mandatos de configuración se activarán cuando reinicie el direccionador.

Entre los mandatos de configuración X.25 en el indicador `X.25 config>`. La Tabla 61 muestra los mandatos.

Tabla 61. Resumen de los mandatos de configuración X.25

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página 10.
Set	Establece las direcciones de nodo local y DDN X.25, el tamaño de ventana para los niveles de paquete, identifica la Personalidad nacional, la MTU y el número máximo de llamadas. Define los rangos de canales PVC y SVC, el número de segundos que un circuito conmutado puede estar desocupado antes que se borre y especifica si un direccionador necesita actuar como DCE (cuando dos direccionadores están conectados directamente sin que intervenga ninguna red X.25) o el método más normal de actuación en un DTE conectado a una red X.25. Establece la velocidad, la codificación, el cronometraje, la clase de productividad y el tipo de cable.
Enable/Disable	Habilita/inhabilita la característica incoming-calls-barred, la característica outgoing-calls-barred, conversiones dinámicas de direcciones DDN y la característica lower-dtr.
National Enable o National Disable	Habilita/inhabilita los parámetros definidos por la configuración de Personalidad nacional.
National Set	Establece los parámetros definidos por la configuración de Personalidad nacional.
National Restore	Restaura la configuración de Personalidad nacional a sus valores por omisión.
Add/Change/Delete	Añade/cambia/suprime una conversión de dirección, una encapsulación de protocolo o una definición de PVC.
List	Lista las conversiones de direcciones definidas, los parámetros de Personalidad nacional, la encapsulación de protocolos o las definiciones de PVC.

Configuración de la interfaz de red X.25

Tabla 61. Resumen de los mandatos de configuración X.25 (continuación)

Mandato	Función
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página 11.

Set

Utilice el mandato **set** para configurar las direcciones de nodos X.25 locales, el número máximo de llamadas, el tamaño de ventana de nivel de trama y de paquete, los canales PVC y SVC de inferior a superior y el tiempo de desocupado para un circuito conmutado.

Sintaxis:

```
set                address . . .  
                   cable  
                   calls-out . . .  
                   clocking . . .  
                   default-window-size . . .  
                   encoding  
                   equipment-type . . .  
                   htf addr . . .  
                   inter-frame-delay . . .  
                   mtu  
                   national-personality . . .  
                   pvc . . .  
                   speed . . .  
                   svc  
                   throughput-class . . .  
                   vc-idle . . .
```

address *direc-nodo-x.25*

Establece la dirección de interfaz X.25 local (*direc-nodo-x.25*). Establezca la dirección de nodo X.25 en 0, no en 00, para suprimir la dirección X.25 local.

Ejemplo: `set address 8982800`

cable *tipo*

Establece el tipo de cable de la manera siguiente:

- RS-232 DTE
- RS-232 DCE
- V35 DTE
- V35 DCE
- V36 DTE
- V36 DCE
- X21 DTE
- X21 DCE

Configuración de la interfaz de red X.25

Se utiliza un cable DTE al conectar el direccionador a algún tipo de dispositivo DCE (por ejemplo, un módem o una DSU/CSU).

Se utiliza un cable DCE cuando el direccionador actúa como DCE y proporciona el cronometraje para la conexión directa.

Notas:

1. Si configura una interfaz en el adaptador EIA 232 de 8 puertos, los únicos tipos de cable que puede configurar son RS-232 DTE y RS-232 DCE.
2. Si está configurando una interfaz en el adaptador V.35/V.36 de 6 puertos, los únicos tipos de cable que puede configurar son V.35 DTE, V.35 DCE, V.36 DTE y V.36 DCE.
3. Si está configurando una interfaz en un adaptador X.21 de 8 puertos, los únicos tipos de cable que puede configurar son X.21 DTE y X.21 DCE.

calls-out *valor*

Establece el número máximo de SVC iniciados localmente, activos simultáneamente.

Valores válidos: De 1 a 239

Valor por omisión: 4

clocking *external o internal*

Para conectar con un módem o DSU, configure el cronometraje externo y seleccione el cable DTE adecuado con el mandato **set cable**. Utilice el mandato **set speed** para configurar la velocidad de línea.

Para conectar directamente con otro dispositivo DTE, configure el cronometraje interno, seleccione el cable DCE adecuado con el mandato **set cable** y configure el cronometraje/velocidad de línea con el mandato **set speed**.

Valor por omisión: external

default-window-size *valor*

Establece el tamaño de ventana para el nivel de paquete asignado por el direccionador si no hay ningún recurso de tamaño de ventana en el paquete de Petición de llamada. El rango lo determina el módulo del paquete de Personalidad nacional (PACKET-EXT-SEQ-MODE).

Valor por omisión: 2

Ejemplo: set default-window-size 3

encoding *NRZ o NRZI*

Establece el esquema de codificación de transmisión HDLC para la interfaz. Puede establecerse la codificación para NRZ (sin retorno a cero) o NRZI (inversión sin retorno a cero). NRZ es el esquema de codificación más ampliamente utilizado mientras que NRZI se utiliza en algunas configuraciones de IBM.

Valor por omisión: NRZ

equipment-type *DCE o DTE*

Especifica si los niveles de trama y de paquete actúan como DCE o DTE. Este mandato no tiene ninguna relación con el tipo de cable que se utiliza.

Valor por omisión: DTE (debe ser DTE para X.31)

Configuración de la interfaz de red X.25

htf addr *direc-nodo-x.25*

Establece la dirección de DTE local cuando se utiliza DDN. Convierte la dirección IP en una dirección X.121 y no como el mandato **set address**, que se utiliza para establecer la dirección de DTE local cuando se utiliza CCITT.

inter-frame-delay *valor*

Este parámetro define el retardo mínimo entre las tramas transmitidas. El establecimiento de este parámetro es útil cuando se intercambia información directamente con un equipo más antiguo. Este parámetro es la período de tiempo entre tramas en segundos.

Nota: Si se configura un retardo entre tramas que no es cero para una interfaz X.25 de un adaptador EIA-232E de 8 puertos, un adaptador V.35/V.36 de 6 puertos o un adaptador X.21 de 8 puertos, se configura la velocidad utilizando el mandato **set speed**.

Valor por omisión: 0

mtu *valor*

Establece la Unidad máxima de transmisión (MTU) en bytes. Se trata del tamaño máximo de mensaje que se entregará a la interfaz X.25 para que se empaquete y transmita a través de una línea serie. El rango es de 576 a 16384.

Valor por omisión: 1500

Si encuentra tiempos de espera excedidos de reensamblaje de paquetes al transferir datos a través de la interfaz X.25, debe determinar cuál es el tamaño mínimo de paquete para todas las interfaces serie o LAN que conducen al punto final y, después calcular una MTU X.25 más adecuada. No debe tomar en consideración directamente el tamaño real de paquete X.25 en este cálculo porque X.25 tiende a utilizar un tamaño de paquete menor. Normalmente, X.25 envía hasta 7 paquetes a la vez antes de esperar un reconocimiento.

Por ejemplo, considere una topología de red que incluya:

- Una LAN de Red en Anillo que tiene un tamaño de paquete de 4000
- Una línea serie X.25 que tiene un tamaño de paquete de 128 con un tamaño de ventana de 7 y una velocidad de bits de 9600 bps.
- Una LAN Ethernet con un tamaño de paquete de 1500

En este caso, probablemente establecería la MTU X.25 en 1500. Esto significa que se enviarán 12 paquetes aproximadamente a través de la interfaz X.25. (MTU / tamaño de paquete X.25 = número de paquetes X.25 que se han de enviar).

Cuando se utilice una MTU de 4096, deben enviarse 32 paquetes a través de la interfaz X.25. ($4000 / 128 = 31,25$). En este caso, se producirán los tiempos de espera excedidos de reensamblaje de paquetes si la velocidad de módem X.25 es de 9600 bps. Probablemente, si utiliza la velocidad de módem X.25 de 56 kbps se resolverá este problema.

Notas:

1. El parámetro MTU tiene un impacto significativo en los requisitos de memoria y en la utilización de memoria del dispositivo. Utilice un valor de MTU de 8192 o inferior para los dispositivos con menos de 8 M de memoria.

Configuración de la interfaz de red X.25

- La cantidad de memoria disponible mientras el dispositivo está en ejecución limita el número de SVC que pueden establecerse a la vez que se mantiene un rendimiento óptimo. Para recomendaciones sobre el número máximo de SVC, consulte la página inicial del producto en la World Wide Web.

national-personality *GTE-Telenet o DDN*

Establece los 28 parámetros por omisión para la Personalidad nacional GTE-Telenet o DDN.

Valor por omisión: GTE-Telenet

pvc low/high *valor*

Define los números de canal de Circuito virtual permanente del inferior al superior. Cero indica que no hay ningún PVC. Por omisión no hay ningún PVC.

pvc low

0

pvc high

0

El rango va de 1 a 4095. Estos valores establecen los límites de un rango de VC determinado. Existe el máximo de 2500 PVC.

Ejemplo: set pvc low 40

Nota: Los valores no deben solapar los valores establecidos para los SVC.

speed *valor-velocidad*

Para el cronometraje interno, utilice este mandato para especificar la velocidad de las líneas de reloj de transmisión y recepción.

Para el cronometraje externo, este mandato no afecta al funcionamiento de la WAN/línea serie pero establece la velocidad que algunos protocolos, como IPX, utilizan para determinar los parámetros de coste de direccionamiento. Debe establecer la velocidad de manera que coincida con la velocidad real de la línea.

Valores válidos:

Cronometraje interno: Consulte la Tabla 62

Cronometraje externo: Consulte la Tabla 63 en la página 474

Nota: El software X.25 sólo está soportado a velocidades de hasta 256 000 bps.

Tabla 62. Velocidades de línea cuando se utiliza el cronometraje interno para interfaces 2216

Tipo de adaptador	Rango de velocidades
EIA 232 de 8 puertos	De 9600 a 64 000 bps
V.35/V.36 de 6 puertos	De 9600 a 460 800 bps, 1 544 000 bps ó 2 048 000 bps
X.21 de 8 puertos	De 9600 a 460 800 bps, 1 544 000 bps ó 2 048 000 bps

Configuración de la interfaz de red X.25

Tabla 63. Velocidades de línea cuando se utiliza el cronometraje externo para interfaces 2216

Tipo de adaptador	Rango de velocidades
EIA 232 de 8 puertos	De 2400 a 64 000 bps
V.35/V.36 de 6 puertos	De 2400 a 2 048 000 bps
X.21 de 8 puertos	De 2400 a 2 048 000 bps

Valor por omisión: 9600

svc low/high inbound o two-way o outbound valor

Define el número de canal de inferior a superior del circuito virtual conmutado. Cuando low=high=0, no hay ningún VC definido en esta categoría.

Ejemplo: set SVC low-two-way 1

Inbound

Especifica el rango de números de canales lógicos que se han de asignar a los SVC de entrada. Por omisión, no hay ningún SVC de sólo entrada.

Valores válidos: De 0 a 4095

Valores por omisión: 0

Two-way

Especifica el rango de números de canales lógicos que se han de asignar a los SVC bilaterales. Por omisión, hay sesenta y cuatro SVC bilaterales.

Valores válidos: De 0 a 4095

Valores por omisión:

svc low

1

svc high

64

Outbound

Especifica el rango de números de canales lógicos que se han de asignar a los SVC de salida. Por omisión, no hay ningún SVC de sólo salida.

Valores válidos: De 0 a 4095

Valor por omisión: 0

Nota: Los valores de cada rango no deben solapar otros rangos de SVC ni rangos de PVC. La Tabla 64 muestra una configuración de VC posible.

Tabla 64. Ejemplo de definiciones de VC

	Low	High
PVC	1	40
inbound	0	0
two-way	41	59
outbound	60	500

Configuración de la interfaz de red X.25

throughput-class inbound o outbound *velocidad-bits*

Define la clase de productividad pedida al realizar una petición de llamada mientras está habilitada la negociación de productividad.

Valor por omisión: 2400 bps

Este valor se pasa por alto al procesar peticiones de llamada de entrada.

vc-idle *valor*

Define el número de segundos que un circuito conmutado puede estar desocupado antes de que el direccionador lo borre. Cero indica que el direccionador nunca borra un circuito desocupado.

Valores válidos: De 1 a 255

Valor por omisión: 30 segundos

Enable

Utilice el mandato **enable** para habilitar las conversiones de direcciones DDN, los restablecimientos de interfaz o las características incoming-calls-barred, outgoing-calls-barred y lower-dtr.

Sintaxis:

enable

ddn—address-translations

Nota: La habilitación de conversiones de dirección ddn ya no está permitida. Esta característica toma por omisión habilitada cuando la personalidad nacional seleccionada es DDN y toma por omisión inhabilitada en todos los demás casos.

incoming-calls-barred

lower-dtr

outgoing-calls-barred

incoming-calls-barred

Especifica que el direccionador no aceptará llamadas de entrada. El valor por omisión para este parámetro es inhabilitado u *off*, que permite las llamadas de entrada.

lower-dtr

Este parámetro determina la forma en que se maneja la señal terminal de datos preparado (DTR) para las interfaces de línea serie alquiladas que están inhabilitadas. Si este parámetro se establece en "inhabilitado" (el valor por omisión), la señal DTR se emitirá cuando se inhabilite la interfaz.

Si *lower-dtr* se establece en "habilitado", el DTR se desactivará cuando la interfaz esté inhabilitada. Este comportamiento puede ser aconsejable en situaciones en las que se ha configurado la interfaz como un enlace alternativo para el Redireccionamiento de WAN y la interfaz está conectada a un módem de marcación de salida que mantiene su conexión de marcación basándose en el estado de la señal DTR.

Cuando *lower-dtr* está habilitado y la interfaz está inhabilitada, la señal DTR se desactiva y el módem mantiene desactivada la conexión de marcación. Cuando la interfaz está habilitada, debido a un escenario de seguridad de Redireccionamiento de WAN, se emite el DTR y el módem marca un número almacenado para el sitio de seguridad. Cuando se

Configuración de la interfaz de red X.25

restaura la interfaz primaria, se inhabilita la interfaz alternativa, el DTR se desactiva y el módem deja en suspenso la conexión de marcación.

Se dan soporte a los tipos de cable siguientes:

RS-232
V.35
V.36

El valor por omisión es inhabilitado.

outgoing-calls-barred

Especifica que el direccionador no permitirá llamadas de salida. El valor por omisión para este parámetro es inhabilitado u *off* que permite llamadas de salida.

Disable

Utilice el mandato **disable** para inhabilitar las conversiones de direcciones DDN, los restablecimientos de interfaces como parte del certificado de la red o las características *incoming-calls-barred* o *outgoing-calls-barred*.

Nota: Si establece DDN como la personalidad nacional, la conversión de direcciones DDN se habilita automáticamente y este parámetro no surte efecto.

Sintaxis:

disable

ddn-address-translations

Nota: La inhabilitación de conversiones de direcciones DDN ya no está permitida. Esta característica toma por omisión habilitada cuando la personalidad nacional seleccionada es DDN y toma por omisión inhabilitada en todos los demás casos.

incoming-calls-barred

lower-dtr

outgoing-calls-barred

National Enable

Utilice el mandato **national enable** para habilitar una característica definida en la configuración de Personalidad nacional.

Sintaxis:

national enable

accept-reverse-charges

bi-cug

bi-cug-outgoing-access

cug

cug-deletion

cug-incoming-access

cug-insertion

cug-outgoing-access

Configuración de la interfaz de red X.25

cug-zero-override

flow-control-negotiation

frame-ext-seq-mode (necesario para X.31)

packet-ext-seq-mode

request-reverse-charges

suppress-calling-addresses

throughput-class-negotiation

truncate-called-addresses

accept-reverse-charges

Acepta las llamadas a cobro revertido durante el establecimiento de llamada. Esta opción no está disponible para DDN.

Valor por omisión de DDN

off

Valor por omisión GTE

on

bi-cug Habilita el recurso de grupo de usuarios cerrado bilateral en este dispositivo. Por omisión, este recurso está inhabilitado.

Nota: No puede añadir ningún CUG bilateral a menos que este parámetro esté habilitado.

bi-cug-outgoing-access

Habilita el recurso CUG bilateral con acceso externo en este dispositivo. Por omisión, este recurso está inhabilitado.

cug Habilita el recurso de grupo de usuarios cerrado en este dispositivo. Por omisión, este recurso está inhabilitado.

Nota: No puede añadir ningún CUG a menos que este parámetro esté habilitado.

cug-deletion

Suprime un recurso CUG de un paquete de llamada recibido de XTP antes de transmitirlo a través de X.25. Por omisión, esta función está inhabilitada.

cug-incoming-access

Habilita el CUG con el recurso de acceso interno en este dispositivo. Por omisión, este recurso está inhabilitado.

cug-insertion

Inserta el número de cug preferido (específico de dirección, específico de protocolo o específico de interfaz) en una petición de llamada recibida por XTP desde la interfaz X.25 antes de transmitir la petición a través de IP. Si ya hay un recurso CUG en el paquete de llamada, no se sustituirá. Por omisión, esta función está inhabilitada.

cug-outgoing-access

Habilita el recurso CUG con acceso externo en este dispositivo. Por omisión, este recurso está inhabilitado.

cug-zero-override

Hace que el recurso de grupo de usuarios cerrado pase por alto cualquier recurso CUG de los paquetes de petición de llamada con un número CUG de 0. Por omisión, esta función está inhabilitada.

Configuración de la interfaz de red X.25

flow-control-negotiation

Habilita la negociación del tamaño de paquete y ventana durante la configuración de llamada de los SVC.

Valor por omisión de DDN

on

Valor por omisión GTE

on

frame-ext-seq-mode

Establece la numeración de la secuencia de capas de trama en el módulo 128 (es decir, de 0 a 127).

Valor por omisión de DDN

off (debe estar activado para X.31)

Valor por omisión GTE

off

packet-ext-seq-mode

Permite que la capa de paquete utilice números de secuencia extendidos (de 0 a 127).

Valor por omisión de DDN

off

Valor por omisión GTE

off

request-reverse-charges

Pide cobros revertidos para todas las llamadas de salida.

Valor por omisión de DDN

off

Valor por omisión GTE

on

suppress-calling-address

Suprime la dirección de origen en los paquetes de llamada.

Valor por omisión de DDN

off

Valor por omisión GTE

off

throughput-class-negotiation

Habilita el registro de la clase de productividad.

Valor por omisión de DDN

off

Valor por omisión GTE

on

truncate-called-addresses

Permite el truncamiento de la dirección DTE llamada al transmitir una llamada a un DTE. Esta opción sólo se aplica a circuitos XTP.

Valor por omisión de DDN

off

Valor por omisión GTE

off

National Disable

Utilice el mandato **national disable** para inhabilitar una característica definida por la configuración de Personalidad nacional.

Sintaxis:

<u>n</u> ational <u>d</u> isable	<u>a</u> cept-reverse-charges
	<u>b</u> i-cug
	<u>b</u> i-cug-outgoing-access
	<u>c</u> ug
	<u>c</u> ug-deletion
	<u>c</u> ug-incoming-access
	<u>c</u> ug-insertion
	<u>c</u> ug-outgoing-access
	<u>c</u> ug-zero-override
	<u>f</u> low-control-negotiation
	<u>f</u> rame-ext-seq-mode
	<u>p</u> acket-ext-seq-mode
	<u>r</u> equest-reverse-charges
	<u>s</u> uppress-calling-addresses
	<u>t</u> hroughput-class-negotiation
	<u>t</u> runcate-called-addresses

National Set

Utilice el mandato **national set** para establecer uno o todos los valores por omisión establecidos en la configuración de Personalidad nacional.

Sintaxis:

<u>n</u> ational <u>s</u> et	<u>c</u> all-req
	<u>c</u> lear-req . . .
	<u>d</u> isconnect-procedure . . .
	<u>d</u> ly-recall-timer . . .
	<u>d</u> p-timer
	<u>f</u> rame-window-size
	<u>n</u> 2-timeouts
	<u>p</u> acket-size . . .
	<u>r</u> eset . . .
	<u>r</u> estart . . .
	<u>m</u> ax-call-retries . . .
	<u>m</u> in-recall
	<u>m</u> in-connect

Configuración de la interfaz de red X.25

collision-timer
standard-version
t1-timer
t2-timer
truncate-called-addr-size

call-req

Especifica el número de intervalos de 10 segundos permitidos antes abandonar una petición de llamada y borrarla. Un cero indica una espera infinita. En una salida del mandato list, se visualiza como el temporizador t21.

Valor por omisión de DDN

20 decasegundos

Valor por omisión GTE

20 decasegundos

clear-req *retries o timer*

Especifica el número de retransmisiones de petición de borrar.

Retries

Número de transmisiones de petición de borrar permitidas antes de que se tome la acción. En una salida del mandato list, se visualiza como la cuenta de reintentos r23.

Valor por omisión de DDN

retries=1

Valor por omisión GTE

retries=1

Timer Número de intervalos de 10 segundos que se han de esperar antes de retransmitir un paquete de petición de borrado. Un cero en el valor del temporizador indica una espera indefinida. En una salida del mandato list, se visualiza como el temporizador t23.

Valor por omisión de DDN

18 decasegundos

Valor por omisión GTE

18 decasegundos

disconnect-procedure *passive o active*

Especifica el tipo de procedimiento de conexión para utilizar al conectarse.

Valor por omisión de DDN

passive

Valor por omisión GTE

passive

Passive

Especifica que el direccionador no inicia las tramas SABM al conectarse.

Active Especifica que el direccionador inicia las tramas SABM al conectarse.

dly-recall-timer

Este mandato no se aplica a XTP ni QLLC. Especifica el tiempo de retardo después de haberse intentado el número máximo de reintentos y

Configuración de la interfaz de red X.25

han fallado. Continuará utilizándose el temporizador min-recall para el retardo entre los intentos de llamada hasta que se exceda el número máximo de reintentos de llamadas. No se intentarán llamadas mientras esté en ejecución el temporizador min-recall o dly-recall. El rango es de 0 a 1080 minutos. Especifique 0 cuando no se utilice el temporizador dly.

Valor por omisión de DDN

0

Valor por omisión GTE

0

Ejemplo: national set dly-recall 30

dp-timer

Especifica el número de milisegundos que el nivel de trama permanece en un estado desconectado. Cero indica la transición inmediata desde la fase desconectada al estado de configuración de enlace.

Valor por omisión de DDN

500 milisegundos

Valor por omisión GTE

500 milisegundos

frame-window-size

Especifica el número de tramas que pueden estar pendientes antes del reconocimiento.

Valor por omisión de DDN

7

Valor por omisión GTE

7

n2-timeouts

Especifica el número de veces que el temporizador de retransmisión (T1) puede caducar antes de reciclar la interfaz.

Valor por omisión de DDN

20

Valor por omisión GTE

20

packet-size *default* o *maximum* o *window*

Especifica el tamaño del paquete.

default

Número de bytes de la parte de datos del paquete. Las opciones posibles son 128, 256, 512, 1024, 2048 y 4096. Este valor se utiliza en ausencia de negociación del tamaño de paquete. *Default* no puede ser mayor que el *maximum*.

Valor por omisión de DDN

128

Valor por omisión GTE

128

maximum

El número máximo de bytes en la parte de datos del paquete. Las opciones posibles son 128, 256, 512, 1024, 2048 y 4096.

Configuración de la interfaz de red X.25

Valor por omisión de DDN

256

Valor por omisión GTE

256

window

Número de tramas I pendientes permitidas antes de que sea necesario el reconocimiento. El rango lo determina el Módulo del paquete Personalidad nacional.

Los parámetros relacionados de configuración son

- Ventana máxima por omisión de protocolo
- Establecer tamaño por omisión de ventana

reset *retries o timer*

Especifica el número de retransmisiones de petición de restablecer.

Ejemplo: national set reset retries 2

retries

Número de transmisiones de petición de restablecer permitidas antes de que se borre la llamada. El rango es de 0 a 255. En una salida del mandato list, se visualiza como la cuenta de reintentos r22.

Valor por omisión de DDN

1

Valor por omisión GTE

1

timer Número de intervalos de 10 segundos que se ha de esperar antes de retransmitir un paquete de petición de restablecer. El rango es de 0 a 255. Un cero en el valor del temporizador indica una espera indefinida. En una salida del mandato list, se visualiza como el temporizador t22.

Valor por omisión de DDN

18 decasegundos

Valor por omisión GTE

18 decasegundos

restart *retries o timer*

Especifica el número de transmisiones de petición de reinicio.

retries

Número de transmisiones de petición de reinicio permitidas antes de que se recicle la interfaz. El rango es de 0 a 255. En una salida del mandato list, se visualiza como la cuenta de reintentos r20.

Valor por omisión de DDN

1

Valor por omisión GTE

1

timer Número de intervalos de 10 segundos que se ha de esperar antes de retransmitir un paquete de petición de reinicio. El rango es de 0 a 255. Un cero en el valor del temporizador indica una espera indefinida. En una salida del mandato list, se visualiza como el temporizador t20.

Configuración de la interfaz de red X.25

Valor por omisión de DDN

18 decasegundos

Valor por omisión GTE

18 decasegundos

max-recall-retries

Este mandato no se aplica a XTP ni QLLC. Especifica cuántos intentos de llamadas (por destino) se realizarán antes de borrar los datos e iniciar el temporizador de llamada de retardo. El número máximo de reintentos de llamada se define en toda una interfaz. Especifique 0 para ningún intento de llamada.

Valor por omisión de DDN

3

Valor por omisión GTE

3

Ejemplo: national set max-call-retries 5

min-recall

Especifica el número mínimo de segundos que se ha de esperar antes de reiniciar una llamada para abrir un SVC. El rango es de 0 a 255 segundos.

Valor por omisión de DDN

10 segundos

Valor por omisión GTE

10 segundos

min-connect

Especifica en segundos, el período mínimo de tiempo que un SVC permanecerá establecido una vez se haya realizado la conexión anulando cualquier condición de error. El rango es de 0 a 255 segundos.

Valor por omisión de DDN

90 segundos

Valor por omisión GTE

90 segundos

collision-timer

Especifica en segundos, el retardo de tiempo especificado antes de reiniciar una llamada para abrir un SVC si el intento original ha dado como resultado una colisión de llamadas. El rango es de 0 a 255 segundos.

Valor por omisión de DDN

10 segundos

Valor por omisión GTE

10 segundos

standard-version

Las opciones son ninguno, v1980, v1984 y v1988.

Valor por omisión de DDN

1984

Valor por omisión GTE

1984

t1-timer

Especifica el tiempo de retransmisión de tramas en segundos. El rango es de 1 a 255.

Configuración de la interfaz de red X.25

Valor por omisión de DDN

4 segundos

Valor por omisión GTE

4 segundos

t2-timer

Especifica el período de tiempo de retardo en segundos antes del reconocimiento de una trama I. Se trata de un parámetro de optimización. Si se establece el temporizador en 0 se inhabilita. El rango es de 0 a 255.

Valor por omisión de DDN

0

Valor por omisión GTE

0

truncate-called-addr-size

Especifica el número de caracteres truncados al final de una dirección llamada. Este parámetro sólo pertenece a circuitos XTP. El rango es de 0 a 10.

Valor por omisión de DDN

2

Valor por omisión GTE

2

National Restore

Utilice el mandato **national restore** para restaurar uno o todos los valores por omisión realizados en la configuración de Personalidad nacional a través de los mandatos **national set**, **national enable** o **national disable**.

Sintaxis:

```
national restore          all  
                           accept-reverse-charges  
                           bi-cug  
                           bi-cug-outgoing-access  
                           call-req  
                           clear-req . . .  
                           cug  
                           cug-deletion  
                           cug-incoming-access  
                           cug-insertion  
                           cug-outgoing-access  
                           cug-zero-override  
                           disconnect-procedure . . .  
                           dp-timer  
                           flow-control-negotiation  
                           frame-ext-seq-mode
```

Configuración de la interfaz de red X.25

- frame-window-size
- min-collision-timer
- min-connect-timer
- min-recall-timer
- network-type . . .
- n2-timeouts
- packet-size . . .
- packet-ext-seq-mode
- request-reverse-charges
- reset . . .
- restart . . .
- standard-version
- suppress-calling-addresses
- throughput-class-negotiation
- t1-timer
- t2-timer
- truncate-called-addresses
- truncate-called-addr-size

Add

Utilice el mandato **add** para añadir una dirección X.121, una dirección X.25 DDN, una configuración de protocolo o una definición de PVC.

Sintaxis:

add address
 bi-cugs
 cugs
 htf-address
 protocol
 pvc

address

Añade una conversión de dirección X.121 para un protocolo soportado en la configuración del direccionador. Las solicitudes que aparecen dependen de la dirección de protocolo que está añadiendo. (Consulte los ejemplos siguientes.) La dirección de protocolo y la dirección X.121 que se están entrando representan el protocolo y la dirección DTE X.121 del DTE remoto que conecta con la interfaz X.25 del direccionador. La correlación de una dirección de protocolo y la dirección X.121 debe ser exclusiva a menos que el protocolo sea APPN o DLSw. Una dirección de protocolo no puede correlacionarse con más de una dirección X.121. Una dirección X.121 específica tampoco puede correlacionarse con más de una dirección de protocolo. Se utiliza el mandato **set address** para establecer la dirección X.25 local. Después de establecer la dirección X.25 local, puede utilizar

Configuración de la interfaz de red X.25

una dirección X.25 remota para la marcación de salida y una dirección remota de entrada opcional para el ID de llamada. Si sólo se entra la dirección remota llamada, se utilizará esta dirección para las llamadas de salida y la verificación de las llamadas de entrada.

Ejemplo: add address

Ejemplo IP:

```
Protocol [IP]? IP
IP Address [0.0.0.0]? 128.185.1.2
Enc Priority 1 []? CC
Enc Priority 2 []? SNAP
Enc Priority 3 []? Null
X.25 Address []? 1234590
Remote address []?
Pref CUG []? 11
CUG (2) []? 12
CUG (3) []? 13
CUG (4) []? 14
CUG (5) []? 15
Pref BI-CUG []? 21
BI-CUG (2) []? 22
BI-CUG (3) []?
```

Ejemplo IPX:

```
Protocol [IP]? IPX
CUD Field Usage (Standard or Proprietary)
IPX Host Number (in hex) []?
Enc Priority 1 []? SNAP
Enc Priority 2 []? Null
X.25 Address []?
Pref CUG []?
Pref Bi-CUG []? 1
BI-CUG (2) []? 3
BI-CUG (3) []?
```

Protocol

Especifica el tipo de protocolo de la correlación de direcciones que está añadiendo. Los valores válidos son APPN, DECnet, DLSw, IP, IPX y VINES. El valor por omisión es IP.

Enc Priority

Determina el tipo de encapsulación, tal como se define en RFC 1356, que se pondrá en el CUD. Para IP, las opciones válidas son CC, SNAP o Null. Para IPX, la opción válida es SNAP o Null.

IP Address

Especifica la dirección IP de destino.

CUD Field Usage

Este campo sólo es para la correlación de direcciones IPX con X.25. Determina cómo se rellena el campo Datos de usuario de llamada (CUD) cuando se reciben paquetes de petición de llamada para IPX. El campo CUD puede ser estándar o propietario. Estándar indica que el uso es multiplexión de protocolo utilizado en RFC 1356. Propietario indica un campo CUD propietario que sólo puede utilizarse con 2216 o con direccionadores compatibles. El valor por omisión es estándar.

IPX Host Number

Especifica el número de sistema principal IPX del destino.

X.25 Address

Especifica la dirección DTE X.121 del DTE remoto que conecta con la interfaz X.25 del direccionador. La longitud máxima de dirección es de 15 dígitos.

Configuración de la interfaz de red X.25

pref cug

Especifica el número del grupo de usuarios cerrado preferido para este DTE. El DTE utiliza este CUG cuando realiza llamadas de salida. **Valores válidos:** Del 0 al 9999

Valor por omisión: Ninguno

Nota: No se le solicitará este valor si no ha habilitado el recurso de grupo de usuarios cerrado utilizando el mandato **national enable**.

CUG Especifica los números de grupos de usuarios cerrados para este DTE. Pueden definirse hasta cinco CUG, incluyendo el CUG preferido. **Valores válidos:** Del 0 al 9999

Valor por omisión: Ninguno

Nota: No se le solicitará este valor si no ha habilitado el recurso de grupo de usuarios cerrado utilizando el mandato **national enable**.

pref bi-cug

Especifica el número de grupos de usuarios cerrados bilaterales para este DTE. El DTE utiliza este CUG cuando realiza llamadas de salida. **Valores válidos:** Del 0 al 9999

Valor por omisión: Ninguno

Nota: No se le solicitará este valor si no ha habilitado el recurso de grupo de usuarios cerrado bilateral utilizando el mandato **national enable**.

bi-cug Especifica los números de grupos de usuarios cerrados bilaterales para este DTE. Pueden definirse hasta cinco CUG. **Valores válidos:** Del 0 al 9999

Valor por omisión: Ninguno

Nota: No se le solicitará este valor si no ha habilitado el recurso de grupo de usuarios cerrado bilateral utilizando el mandato **national enable**.

cugs Especifica el número de grupos de usuarios cerrados para esta interfaz X.25. **Valores válidos:** Del 0 al 9999

Valor por omisión: Ninguno

Nota: No se le solicitará este valor si no ha habilitado el recurso de grupo de usuarios cerrado utilizando el mandato **national enable**.

Ejemplo:

```
add cugs
Pref CUG [ ]? 23
CUG (2) [ ]? 24
CUG (3) [ ]? 25
CUG (4) [ ]? 26
CUG (5) [ ]? 27
```

pref cug

Especifica el número del grupo de usuarios cerrado preferido para

Configuración de la interfaz de red X.25

este DTE. El DTE utiliza este CUG cuando realiza llamadas de salida. **Valores válidos:** Del 0 al 9999

Valor por omisión: Ninguno

Nota: No se le solicitará este valor si no ha habilitado el recurso de grupo de usuarios cerrado utilizando el mandato **national enable**.

cug Especifica los números de grupos de usuarios cerrados para este DTE. Pueden definirse hasta cinco CUG. **Valores válidos:** Del 0 al 9999

Valor por omisión: Ninguno

Nota: No se le solicitará este valor si no ha habilitado el recurso de grupo de usuarios cerrado utilizando el mandato **national enable**.

bi-cugs

Especifica el número de grupos de usuarios cerrados para este DTE. **Valores válidos:** Del 0 al 9999

Valor por omisión: Ninguno

Nota: No se le solicitará este valor si no ha habilitado el recurso de grupo de usuarios cerrado utilizando el mandato **national enable**.

Ejemplo:

```
add bi-cugs
Pref BI-CUG [ ]? 23
BI-CUG (2) [ ]? 24
BI-CUG (3) [ ]? 25
BI-CUG (4) [ ]? 26
BI-CUG (5) [ ]? 27
```

pref bi-cug

Especifica el número del grupo de usuarios cerrado preferido para este DTE. El DTE utiliza este BI-CUG al realizar llamadas de salida. **Valores válidos:** Del 0 al 9999

Valor por omisión: Ninguno

Nota: No se le solicitará este valor si no ha habilitado el recurso de grupo de usuarios cerrado bilateral utilizando el mandato **national enable**.

bi-cug Especifica los números de grupos de usuarios cerrados para este DTE. Pueden definirse hasta cinco BI-CUG. **Valores válidos:** Del 0 al 9999

Valor por omisión: Ninguno

Nota: No se le solicitará este valor si no ha habilitado el recurso de grupo de usuarios cerrado bilateral utilizando el mandato **national enable**.

htf-address

Añade una conversión de dirección X.25 de Defense Data Network (DDN).

Ejemplo:

```
add htf-address
Protocol [IP]
Convert HTF address
```

Protocol

Especifica el protocolo que está ejecutando en la interfaz X.25. DDN sólo soporta IP.

Convert HTF address

Convierte la dirección de protocolo en una dirección X.121 de destino en formato Host Table Format (HTF). Consulte también `ddn-address-translations` en la sección de los mandatos Enable/Disable.

protocol

Habilita la encapsulación de un protocolo y define los parámetros asociados.

Ejemplo:

```
add protocol
Protocol [IP]?
Window Size [2]?
Default Packet Size [128]?
Maximum Packet Size [256]?
Circuit Idle Time [30]?
Max VCs [4]?
Pref CUG []? 1
CUG (2) []? 2
CUG (3) []? 3
CUG (4) []? 4
CUG (5) []? 5
Pref BI-CUG []? 11
BI-CUG (2) []? 12
BI-CUG (3) []? 13
BI-CUG (4) []? 14
BI-CUG (5) []? 15
```

Ejemplo QLLC:

```
X.25 Config> add prot
Protocol [IP]? d1s
Idle timer [30]?
QLLC response timer (in decaseconds) [2]?
QLLC response count [3]?
Accept Reverse Charges [N]?
Request Reverse Charges [N]?
Station Type (1) PRI (2) SEC (3) (PEER) [3]?
Max Packet Size [128]?
Packet window size [7]?
Max Message Size [1500]?
Call User Data (in hex, 0 for null) []?
Pref CUG []? 20
CUG (2) []? 21
CUG (3) []?
Pref BI-CUG []?
```

Protocol

Especifica los parámetros de encapsulación de protocolo que desea añadir: APPN, XTP, IP, DECnet, IPX, DLSw o Banyan VINES. El valor por omisión es IP.

Window Size

Especifica el tamaño máximo de ventana de paquete negociable, el número de paquetes que pueden estar pendientes antes de que sea necesaria la confirmación de paquetes. El valor por omisión es 2. El tamaño de ventana puede negociarse a la baja hasta 1 por el DTE llamado.

Los parámetros de configuración relacionados son:

Configuración de la interfaz de red X.25

- Set Default Window

Default Packet Size

Especifica el tamaño por omisión de paquete pedido para los SVC. Este valor sirve de tamaño mínimo de paquete negociable y debe ser igual o menor que el tamaño máximo de paquete especificado con el mandato **national set packet-size**. El *tamaño máximo de paquete por omisión* es de 4096 bytes. El valor por omisión para este parámetro es de 128 bytes.

Los parámetros de configuración relacionados son:

- Valor por omisión de tamaño de paquete de National Set
- Tamaño máximo de paquete de National Set

Maximum Packet Size

Especifica el tamaño máximo de paquete negociable para los SVC. Este valor debe ser igual o menor que el tamaño máximo de paquete especificado con el mandato **national set packet-size**. El valor por omisión para este parámetro es 256 bytes. El valor máximo que puede configurarse para este parámetro es 4096 bytes. Este valor se utiliza en el cálculo del tamaño máximo de trama para esta interfaz X.25.

Los parámetros de configuración relacionados son:

- Valor por omisión de tamaño de paquete de National Set
- Tamaño máximo de paquete de National Set

Circuit Idle Time

Especifica el número de segundos que un SVC puede estar desocupado antes de que el direccionador lo borre. El rango es de 0 a 65365. El valor por omisión es de 30 segundos. Un 0 (cero) especifica que el direccionador nunca borra el circuito.

Maximum VCs

Especifica el número máximo de circuitos que están abiertos en la misma dirección DTE para un protocolo. Consulte RFC 1356 para obtener información sobre la utilización de este parámetro. El rango válido es de 1 a 10. El valor por omisión es 4.

pref CUG, CUG, pref bi-cug, bi-cug

Consulte el mandato **add address**.

Los siguientes son los parámetros exclusivos QLLC:

QLLC response timer

El número de segundos que se ha de esperar un paquete de respuesta Q antes de la retransmisión.

QLLC response count

El número máximo de veces que QLLC retransmitirá. Cuando se agota este número de reintentos, se notifica a la capa superior, lo que puede provocar que el direccionador borre o restablezca el circuito.

Accept Reverse Charges

Permite que este protocolo altere temporalmente el valor del parámetro de Personalidad nacional. Esto no afecta al parámetro de Personalidad nacional.

Configuración de la interfaz de red X.25

Request Reverse Charges

Permite que este protocolo altere temporalmente el valor del parámetro de Personalidad nacional. Esto no afecta al parámetro de Personalidad nacional.

Station Type

Especifica el tipo de estación por omisión para este protocolo:

Pri Estación primaria

Sec Estación secundaria

Peer Estación similar

Max message size

El tamaño máximo de mensaje para este protocolo. Especifique un valor que sea menor o igual al tamaño de MTU máxima de la interfaz.

Call User Data

Especifica el campo CUD por omisión utilizado en paquetes de llamada para este protocolo. Especifique de 1 a 16 caracteres. Si no especifica caracteres, se utiliza el valor por omisión 0xC3.

pvc Añade definiciones de PVC, tamaño de ventana y tamaño de paquete.

Ejemplo: add pvc

Ejemplo IP:

```
Protocol [IP]? IP
Packet Channel Range Start [1]?
Destination X.25 Address [ ]?
Packet Channel Range End [1]?
Window Size [2]?
Packet Size [128]?
```

Protocol

Especifica la encapsulación de protocolo que desea modificar: APPN, XTP, DECnet, Banyan Vines, DLSw, IP o IPX. El valor por omisión es IP.

Packet Channel Range Start

Especifica el número de circuito inicial de este rango de PVC.

Packet Channel Range End

Especifica el número del último circuito de este rango de PVC. Toma el valor por omisión de Packet Channel Range Start.

Destination X.25 Address

Especifica la dirección X.25 del destino del PVC.

Remote Address

Especifica la dirección remota para el ID del llamador en las llamadas recibidas.

Window Size

Especifica el número de paquetes que pueden estar pendientes antes de necesitar confirmación de paquetes. El valor por omisión es 2.

Los parámetros de configuración relacionados son:

- Set Default Window

Packet Size

Especifica el tamaño máximo de paquete negociable para los PVC.

Configuración de la interfaz de red X.25

Este valor debe ser igual o menor que el tamaño máximo de paquete especificado con el mandato **national set packet-size**. El valor por omisión para este parámetro es de 128 bytes. El valor máximo que puede configurarse para este parámetro es 4096 bytes. El máximo para X.31 es 256 bytes. Este valor se utiliza en el cálculo del tamaño máximo de trama para esta interfaz X.25.

Los parámetros de configuración relacionados son:

- Valor por omisión de tamaño de paquete de Nat Set
- Tamaño máximo de paquete de Nat Set

Change

Utilice el mandato **change** para cambiar una dirección X.121, una dirección X.25 DDN, una configuración de protocolo o una definición de PVC.

Nota: Para cambiar una dirección IP que está asociada con una dirección X.121, debe suprimir el registro que contiene la correlación de direcciones y, después, volver a definir la correlación de direcciones.

Sintaxis:

```
change                address  
                        htf-address  
                        protocol  
                        pvc
```

address

Modifica una conversión de direcciones X.121. Las solicitudes que aparecen dependen del protocolo que se cambie.

Ejemplo: change address

Ejemplo IP:

```
Protocol [IP] IP  
IP Address [0.0.0.0]?  
Enc Priority []?  
X.25 Address [00000124040000]?
```

Ejemplo IPX:

```
Protocol [IP] IPX  
CUD Field Usage (Standard or Proprietary) [Standard]?  
IPX Host number (in hex) []?  
Enc Priority []?  
X.25 Address [00000124040000]?
```

htf address

Cambia una conversión de dirección X.25 de Defense Data Network (DDN).

Ejemplo:

```
change htf-address  
Protocol [IP]  
Change HTF address [0.0.0.0]?  
New HTF address [10.4.0.124]?
```

protocol

Cambia una definición de configuración de protocolo.

Ejemplo:

```
change protocol  
Protocol [IP]  
Window Size [2]
```

Configuración de la interfaz de red X.25

```
Default Packet Size [128]
Maximum Packet Size [256]
Circuit Idle Time [30]
Maximum VCs [6]
```

Ejemplo QLLC:

```
X.25 Config> change prot
Protocol [IP]? dls
Idle Timer [30]?
QLLC response timer (in decaseconds) [15]?
QLLC response count [255]?
Accept Reverse Charges [N]?
Request Reverse Charges [N]?
Station Type (1) PRI (2) SEC (3) PEER [3]?
Max Packet Size [256]?
Packet Window size [7]?
Max message size [2048]?
Call User Data (in HEX, 0 for Null) []? C3010000525450
```

pvc Cambia las definiciones de PVC, tamaño de ventana y tamaño de paquete.

Nota: Para cambiar el protocolo, el canal de paquete o la dirección X.25 de destino, debe suprimir el registro que contiene la definición y después volverlo a añadir con los parámetros cambiados. El cambio se aplicará a *todos* los PVC del rango de circuitos definidos por el parámetro Packet Channel Range Start.

Ejemplo:

```
change pvc
Protocol [IP]? IP
Packet Channel Range Start[1]?
Destination X.25 Address [ ]?
Packet Channel Range End [1]
Window Size [2]?
Packet Size [128]?
```

Delete

Utilice el mandato **delete** para suprimir una dirección X.121, una definición de configuración de protocolo o una definición de PVC.

Sintaxis:

```
delete          address
                  bi-cugs
                  cugs
                  protocol . . .
                  pvc
```

address

Suprime una conversión de direcciones X.121.

Ejemplo: delete address

Ejemplo IP:

```
Protocol [IP]?
IP Address [0.0.0.0]?
```

Ejemplo IPX:

```
Protocol [IP]? IPX
IPX Host Number (in hex) [2]?
```

Configuración de la interfaz de red X.25

bi-cugs

Suprime un número de grupo de usuarios cerrado bilateral utilizado por esta interfaz.

Valores válidos:

Y Suprime el CUG actual.

N No suprime el CUG actual.

ALL Suprime todos los CUG restantes.

Q Detiene la supresión de cualquier CUG que quede.

Ejemplo:

```
delete bi-cugs
Delete Pref BI-CUG [Y]?
Delete BI-CUG (2) [Y]? N
Delete BI-CUG (3) [Y]? q
```

cugs Suprime los números de grupos de usuarios cerrados que utiliza esta interfaz. Este mandato funciona de manera similar al mandato **delete bi-cug**.

Ejemplo:

```
del cug

Delete Pref CUG [Y]?
Delete CUG (2) [Y]?
Delete CUG (3) [Y]? q
```

protocol *tipo-protocolo*

Suprime una definición de configuración de encapsulación de protocolo. *tipo-protocolo* es el nombre o número de la encapsulación de protocolo que está definida actualmente en la configuración del direccionador.

pvc Suprime una definición de PVC. Se suprimirán *todos* los PVC del rango de circuitos definido por el parámetro Packet Channel Range Start.

Ejemplo:

```
delete pvc
Protocol [IP]?
Destination X.25 Address [ ]?
Packet Channel Range Start [ ]?
```

List

Utilice el mandato **list** para visualizar la configuración actual para el parámetro especificado.

Sintaxis:

```
list
address
all
cugs
detailed
protocols
pvc
summary
```

address

Lista todas las conversiones de direcciones X.121.

Configuración de la interfaz de red X.25

Ejemplo:

list address

```
IF#      Prot #      Active Enc      Protocol ->      X.25 address
1        0(IP)        CC            10.1.2.3 ->      1238765742
1        7(IPX)        SNAP         10             ->      12389
                CUGS: 11 12 13 14 15      BI-CUGS: 21 22
```

- all** Lista todas las direcciones X.25, parámetros de Personalidad Nacional, todos los protocolos definidos y sus valores y todos los PVC definidos.

Ejemplo:

list all

X.25 Configuration Summary

```
Node Address:      313131
Max Calls Out:     4
Inter-Frame Delay: 0      Encoding: NRZ
Speed:             64000   Clocking: Internal
MTU:               2048    Cable: V.35 DCE
Lower DTR:         Disabled
Default Window:    2      SVC idle: 30 seconds
National Personality: GTE Telenet (DTE)
PVC                low: 1   high: 1
Inbound            low: 0   high: 0
Two-Way            low: 2   high: 64
Outbound           low: 0   high: 0
Throughput Class in bps Inbound: 2400
Throughput Class in bps Outbound: 2400
```

X.25 National Personality Configuration

```
Request Reverse Charges: on Accept Reverse Charges: on
Frame Extended seq mode: off Packet Extended seq mode: off
Incoming Calls Barred: off Outgoing Calls Barred: off
Throughput Negotiation: on Flow Control Negotiation: on
Suppress Calling Addresses: off DDN Address Translation: off
Truncate Called Addresses: off
Number of digits to truncate called addresses to: 2
CUG Support: off BI-CUG Support: off
CUG Outgoing Access: off CUG Incoming Access : off
BI-CUG Outgoing Access: off CUG 0 Override: off
CUG Isertion: off CUG deletion: off
Call Request Timer: 20 decaseconds
Clear Request Timer: 18 decaseconds (1 retries)
Reset Request Timer: 18 decaseconds (1 retries)
Restart Request Timer: 18 decaseconds (1 retries)
Min Recall Timer 10 seconds
Min Connect Timer 90 seconds
Collision Timer 5 seconds
T1 Timer: 4.00 seconds N2 timeouts: 20
T2 Timer: 2.00 seconds DP Timer: 500 milliseconds
Standard Version: 1984 Network Type: CCITT
Disconnect Procedure: passive
Window Size Frame: 7 Packet: 2
Packet Size Default: 128 Maximum: 256
```

X.25 protocol configuration

No protocols defined

X.25 PVC configuration

No PVCs defined

X.25 address translation configuration

No address translations defined

- cugs** Lista los números de CUG y BI-CUG para cada interfaz X.25 de este dispositivo.

Ejemplo:

li cugs

```
CUGS: 23 24 25 26 27
```

Configuración de la interfaz de red X.25

detailed

Lista el valor de todos los parámetros por omisión que el mandato **national set** modifica. Se listan descripciones de la visualización de pantalla en el mandato **national set** que se describe más adelante en este capítulo.

Ejemplo:

list detail

X.25 National Personality Configuration

```
Follow CCITT: on      OSI 1984:  on      OSI 1988:  off
Request Reverse Charges: off  Accept Reverse Charges:  off
Frame Extended seq mode: off  Packet Extended seq mode: off
Incoming Calls Barred:  off  Outgoing Calls Barred:  off
Throughput Negotiation: on   Flow Control Negotiation: off
Suppress Calling Addresses: off  DDN Address Translation:  off
Truncate Called Addresses: off
Number of digits to truncate called address to: 2
CUG Support: off        BI-CUG Support: off
CUG Outgoing Access: off  CUG Incoming Access : off
BI-CUG Outgoing Access: off  CUG 0 Override: off
CUG Insertion: off      CUG deletion: off
T21 (Call Request Timer): 20 decaseconds
T23 (Clear Request Timer): 18 decaseconds (1 retries)
T22 (Reset Request Timer): 18 decaseconds (1 retries)
T20 (Restart Request Timer): 18 decaseconds (1 retries)
Min Recall Timer: 10 seconds
Min Connect Timer: 90 seconds
Collision Timer: 8 seconds
T1 Timer: 4.00 seconds  N2 timeouts: 20
T2 Timer: 0.00 seconds  DP Timer: 500 milliseconds
Standard Version: 1984  Network Type: CCITT
Disconnect Procedure: active
Window Size  Frame: 7  Packet: 2
Packet Size  Default: 256  Maximum: 256
```

protocols

Lista todas las configuraciones de protocolo definidas. Consulte la sección "Add" en la página 485 para ver una descripción de los parámetros.

Ejemplo:

list protocols

X.25 protocol configuration

Protocol Number	Window Size	Packet-Size Default	Packet-Size Maximum	Idle Time	Max VCs
0(IP)	2	128	256	30	4
	CUGS: 11 12 13 14 15			BI-CUGS: 21 22	

QLLC Protocols

Protocol Number	Packet Window	Packet MaxSize	Idle Time	Response Timer	Response Count	Reverse Charges Accept	Reverse Charges Request	Max Message	Station Type
26(DLSW)	7	256	30	15	255	N	N	2048	PEER
	CUD : [C3 01 00 00 52 54 50]								
	CUGS: 11 12 13 14 15			BI-CUGS: 21 22					

pvc Lista todos los PVC definidos.

Ejemplo:

list pvc

X.25 PVC configuration

Prtcl	X.25 Address	Active Enc	Window	Pkt_len	Pkt_chan
0	8383838383	CC	4	1024	3 - 3

summary

Lista todos los valores establecidos por los mandatos **set** y **enable**. Estos valores modifican la configuración X.25.

Ejemplo:

list summary

X.25 Configuration Summary

```
Node Address:      313131
Max Calls Out:     4
Inter-Frame Delay: 0      Encoding: NRZ
Speed:             64000   Clocking: Internal
MTU:               2048    Cable: V.35 DCE
Lower DTR:         Disabled
Default Window:    2      SVC idle: 30 seconds
National Personality: GTE Telenet (DTE)
PVC               low: 1   high: 1
Inbound           low: 0   high: 0
Two-Way           low: 2   high: 64
Outbound          low: 0   high: 0
Throughput Class in bps Inbound: 2400
Throughput Class in bps Outbound: 2400
```

Acceso al proceso de supervisión de interfaces

Para supervisar la información relacionada con la interfaz de red X.25, acceda al proceso de supervisión de interfaz de la manera siguiente:

1. En el indicador OPCON, entre **talk 5**. Por ejemplo:

```
* talk 5
+
```

Se visualiza el indicador GWCON (+) en la consola. Si no aparece el indicador cuando entre en GWCON, pulse **Intro** de nuevo.

2. En el indicador GWCON, entre el mandato **configuration** para ver los protocolos y las redes para los que está configurado el direccionador. Por ejemplo:

```
+ configuration
```

Consulte la página "Configuration" en la página 120 para ver un ejemplo de salida del mandato **configuration**.

3. Entre el mandato **network** y el número de interfaz X.25.

```
+ network 2
X.25>
```

Se visualiza el indicador de supervisión X.25 en la consola. Puede ver la información acerca de la interfaz X.25 entrando los mandatos de supervisión X.25.

Mandatos de supervisión X.25

Esta sección resume y explica todos los mandatos de supervisión X.25. Los mandatos de supervisión X.25 le permiten ver los parámetros y las estadísticas de las interfaces y las redes que transmiten paquetes X.25. Los mandatos de supervisión visualizan los valores de configuración para los niveles físico, de trama y de paquete. También tiene la opción de visualizar los valores para todos los niveles de protocolo a la vez.

Entre los mandatos de supervisión X.25 en el indicador X.25>. La Tabla 65 en la página 498 muestra los mandatos.

Configuración de la interfaz de red X.25

Tabla 65. Resumen de los mandatos de supervisión X.25

Mandato de supervisión	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página 10.
List	Lista las estadísticas individuales de PVC o SVC y la información general.
Parameters	Visualiza los parámetros actuales para cualquier nivel de la configuración X.25.
Reset	Restablece los temporizadores dly-recall y min-recall para todos los similares de esta interfaz o restablece los temporizadores para un destino específico entrando la dirección de destino X.25. Esto permitirá que la secuencia de llamada vuelva a empezar.
Statistics	Visualiza las estadísticas actuales para cualquier nivel de configuración X.25.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página 11.

List

Utilice el mandato **list** para visualizar los PVC y SVC activos actualmente.

Sintaxis:

list pvcs
svcs

pvc Visualiza los circuitos virtuales permanentes configurados.

svc Visualiza los circuitos virtuales conmutados activos.

Ejemplo:

```
list svc
```

LCN/ State	Destination Address	Originate Call	Transmits Queued	Protocol Encapsulated	Totals Xmts	Rcvs	Resets
13 D	898280077113	YES	0	IP	8943	261	1
20 D	898280077114	NO	0	IP	943	43	0
42 P	898280077116	YES	6	IP	0	0	0
23 C	898280077117	YES	0	IP	3054	110	0

D - Data Transfer P - Call Progressing
C - Call Clearing

Parameters

Utilice el mandato **parameters** para visualizar los parámetros actuales para cualquier nivel de la configuración X.25.

Sintaxis:

parameters all
frame
packet
physical

all Visualiza los parámetros para los niveles de paquete, trama y físico.

frame Visualiza los parámetros para el nivel de trama.

Ejemplo:

```
parameters frame
Frame Layer Parameters:
Maximum Frame Size = 262 Maximum Window Size = 7
Protocol Enabled = YES Equipment Type = DTE
T1 Retransmit Timer = 4 T2 Acknowledge Timer = 2
N2 Retry Counter = 20 Disconnect Procedure = PASSIVE
Disconnect Timer = 500 Network Type = GTE
Protocol Options: Inhibit Idle RRs No MOD 128 NO Enable SARM NO
```

packet

Visualiza los parámetros para el nivel de paquete.

Ejemplo:

```
parameters packet
Packet Layer Parameters:
Default Packet Size = 128 Maximum Packet Size = 256
Log 2 Packet size = 2 Acknowledge Delay = 0
Layer Enabled = YES Default Window Size = 2
Lowest SVC = 1 Highest SVC = 64
Lowest PVC = 0 Highest PVC = 0
T20 (Restart) = 18 R20 (Retry) = 1
T21 (Call) = 20
T22 (Reset) = 18 R22 (Retry) = 1
T23 (Clear) = 18 R23 (Retry) = 1
Network Type = GTE Equipment Type = DTE
```

physical

Visualiza los parámetros para el nivel físico.

Ejemplo:

```
parameters physical
Physical Layer Parameters:
Interface Type = V.35

Maximum Frame Size = 264 InterFrame Delay = 2
Configured Speed = 0 Clocking = External
Encoding = NRZ
Protocol Enabled = Yes
```

Reset

Utilice el mandato **reset** para restablecer los temporizadores dly-recall o min-recall y reiniciar los intentos de llamada para todos los destinos X.25 o para un destino X.25 en particular.

Sintaxis:

```
reset                all-peer-recall-tmrs
                    peer-recall-tmr
```

all-peer-recall-tmrs

Restablece la secuencia de llamadas para todos los destinos X.25 (similares) de esta interfaz. Por lo tanto, si un destino estaba en dly-recall, puede utilizarse para restablecer el temporizador y volver a empezar la secuencia.

Ejemplo: reset all-peer

Este mandato devolverá uno de los mensajes siguientes:

- Reset delay recall timers completed.
- No recall timers running for this net.
- No peers located for this net.

peer-recall-tmr

Restablece la secuencia de llamadas para un destino X.25 (similar) en particular de esta interfaz. Entre el destino X.25 que se ha de restablecer.

Ejemplo 1: reset peer-recall-tmr

Configuración de la interfaz de red X.25

```
reset peer-recall-tmr
Enter X.25 address: 89828007713
```

Este mandato devolverá uno de los mensajes siguientes:

- Reset delay recall timers completed.
- No recall timers running for this net.

Ejemplo 2: reset peer-recall-tmr 89828007713

```
reset peer-recall-tmr 89828007713
```

Este mandato devolverá uno de los mensajes siguientes:

- Reset delay recall timers completed.
- No recall timers running for this net.

Statistics

Utilice el mandato **statistics** para visualizar las estadísticas actuales de cualquier nivel de configuración X.25.

Sintaxis:

statistics

all

frame

packet

physical

all Visualiza las estadísticas para los niveles de paquete, trama o físico.

frame Visualiza las estadísticas para el nivel de trama.

Ejemplo:

```
statistics frame
Frame Layer Counters:      Received      Transmitted
Information Frames         0              0
RR Command                 0              0
RR Response                0              0
RNR Command               0              0
RNR Response              0              0
REJ Command                0              0
REJ Response              0              0
SABM                      0              71
SABME                     0              0
UA                        0              0
DISC                      0              0
DM                        0              0
FRMR                      0              0
Total Bytes                0              0
Frame Layer Miscellaneous:
Queued Output Frames = 0 Protocol Layer State = Link Setup
Send Sequence N(S)   = 0 Receive Sequence N(R) = 0
```

packet

Visualiza las estadísticas para el nivel de paquete.

Ejemplo:

```
statistics packet
Packet Counters:          Received      Transmitted
Call Request              0              0
Call Accepted             0              0
Clear Request             0              0
Clear Confirm             0              0
Interrupt Request         0              0
Interrupt Confirm         0              0
RR Packet                 0              0
RNR Packet                0              0

Reset Request             0              0
Reset Confirm             0              0
```

Configuración de la interfaz de red X.25

```
Restart Request          0          0
Restart Confirm         0          0
Diagnostic               0          0
Data Packet             0          0
Data Bytes              0          0
Buffers Queued          0          0
Invalid Packets Received = 0
Switched Circuits Opened = 0
```

physical

Visualiza las estadísticas para el nivel físico.

Ejemplo:

```
statistics physical
X.25 Physical Layer Counters:
Rx Bytes          0  Tx Bytes          0

Adapter cable:      V.35 DTE

Nicknames:  RTS CTS DSR DTR DCD
PUB 41450:  CA  CB  CC  CD  CF
State:      ON  ON  ON  ON  ON

Line speed:          unknown
Last port reset:    12 minutes, 21 seconds ago

Input frame errors:
CRC error           0  alignment (byte length)  0
missed frame        0  too long (> 0 bytes)    0
aborted frame       0  DMA/FIFO overrun        0
Output frame counters:
DMA/FIFO underrun errors  0  Output aborts sent      0
```

Interfaces de red X.25 y el mandato interface de GWCON

Aunque las interfaces X.25 tienen sus propios procesos para la supervisión, el direccionador también visualiza estadísticas completas para las interfaces de red instaladas cuando se utiliza el mandato **interface** desde el entorno GWCON. (Para obtener más información sobre el mandato **interface**, consulte la sección Capítulo 8. El proceso de operación/supervisión (GWCON - Talk 5) y sus mandatos).

Estadísticas visualizadas para las interfaces X.25

Cuando se ejecuta el mandato **interface** desde el entorno GWCON para interfaces X.25, se visualizan las estadísticas siguientes:

```
+interface 11
Nt Nt' Interface Slot-Port Self-Test Self-Test Maintenance
11 11 X25/0 Slot: 8 Port: 1 Passed Failed Failed
1 0 0

X.25 MAC/data-link on V.35/V.36 interface
Interface State: DCD CTS Packet Layer Frame Layer
ON ON UP UP
Packet Counters: Received Transmitted
Data Packet 0 353
Data Bytes 0 18888
Buffers Queued 0 0
Invalid Packets Received = 0
Switched Circuits Opened = 0

Frame Layer Counters: Received Transmitted
Information Frames 354 354

X.25 Physical Layer Counters:
Rx Bytes 3316 Tx Bytes 22204

Adapter cable: V.35 DTE

V.24 circuit: 105 106 107 108 109
Nicknames: RTS CTS DSR DTR DCD
PUB 41450: CA CB CC CD CF
State: ON ON ON ON ON

Line speed: 64.000 kbps
```

Configuración de la interfaz de red X.25

```
Last port reset:          1 hour, 20 minutes, 25 seconds ago

Input frame errors:
CRC error                 0 alignment (byte length)      0
missed frame             0 too long (> 2057 bytes)      0
aborted frame           0 DMA/FIFO overrun             0
Output frame counters:
DMA/FIFO underrun errors 0 Output aborts sent          0
Interface buffer pool: Total = 57, Free = 56
```

La lista siguiente describe las estadísticas de interfaz:

Nt Número de interfaz global

Nt ' Reservado para uso futuro del circuito de marcación

Interface

Nombre y número de interfaz (dentro de las interfaces del mismo tipo)

Slot Número de ranura de interfaz

Port Número de puerto de interfaz

Self-Test Passed

Número de veces que la autoprueba ha sido satisfactoria

Self-Test Failed

Número de veces que la autoprueba ha fallado

Maintenance Failed

Número de anomalías de mantenimiento

Interface state

Visualiza el estado actual de las señales de control de módem de entrada, la capa de paquete (X.25 capa 3) y la capa de trama (X.25 capa 2).

Packet Counters

Proporciona estadísticas sobre los paquetes recibidos y transmitidos.

Data Packets

Visualiza el número de paquetes de datos que la interfaz transmite y recibe en la red.

Data Bytes

Visualiza el número de bytes de datos que la interfaz transmite y recibe en la red.

Buffers Queued

Visualiza el número de almacenamientos intermedios que actualmente están en cola para su transmisión en la red. Estos pueden ser mensajes de supervisión de la capa de trama o de paquete así como paquetes del reenviador.

Invalid Packets Received

Visualiza el número de paquetes X.25 no válidos recibidos de la red.

Switched Circuits Open

Visualiza el número de circuitos conmutados abiertos actualmente.

Frame Layer Counters

Proporciona las estadísticas generadas a partir de los contadores de Capa de trama.

Information Frames

Visualiza el número de tramas de información X.25 que la interfaz ha transmitido o recibido.

Configuración de la interfaz de red X.25

X.25 Physical Layer Counters

Proporciona las estadísticas generadas a partir de los contadores de Capa física.

RX Bytes

Visualiza el número de bytes recibidos por la Capa física.

TX Bytes

Visualiza el número de bytes transmitidos por la Capa física.

Line speed

La velocidad de reloj de transmisión.

Last port reset

El período de tiempo desde el último restablecimiento de puerto.

Input frame errors:

CRC error

El número de paquetes recibidos que contenían errores de suma de comprobación y como consecuencia de ello se han eliminado.

Alignment

El número de paquetes recibidos que no eran un número par de 8 bits de longitud y como consecuencia de ello se han eliminado.

Too short

El número de paquetes que tenían menos de 2 bytes de longitud y como consecuencia de ello se han eliminado.

Too long

El número de paquetes mayores que el tamaño configurado y como resultado de ello se han eliminado.

Aborted frame

El número de paquetes recibidos que se han cancelado anormalmente por el emisor o un error de línea.

DMA/FIFO overrun

El número de veces que la tarjeta de interfaz serie no ha podido enviar datos con la suficiente rapidez para que la memoria del almacenamiento intermedio de paquetes del sistema los recibiese de la red.

Missed frame

Cuando una trama llega al dispositivo y no hay ningún almacenamiento intermedio disponible, el hardware elimina la trama e incrementa el contador de tramas que faltan.

L & F bits not set

En interfaces serie, el hardware establece información de descriptor de entrada para las tramas que llegan. Si el almacenamiento intermedio puede aceptar la trama completa en la llegada, el hardware establece el primer y último bit de la trama, lo que indica que el almacenamiento intermedio ha aceptado toda la trama. Si no se establece alguno de estos bits, se elimina el paquete, se incrementa el contador L & F bits not set y se borra el almacenamiento intermedio para reutilización.

Nota: No es probable que el contador L & F bits not set se vea afectado por el tráfico.

Output frame counters:

Configuración de la interfaz de red X.25

DMA/FIFO underrun errors

El número de veces que la tarjeta de interfaz serie no ha podido recuperar datos con la suficiente rapidez de la memoria de almacenamiento intermedio de paquetes del sistema para transmitirlos en la red.

Output aborts sent

El número de transmisiones que se han cancelado anormalmente como petición del software de nivel superior.

Soporte de la reconfiguración dinámica de la interfaz de red X.25

Esta sección describe la reconfiguración dinámica (DR) en la medida en que afecta a los mandatos Talk 6 y Talk 5.

Delete Interface de CONFIG (Talk 6)

La interfaz de red X.25 soporta el mandato **delete interface** de CONFIG (Talk 6) sin ninguna restricción.

Activate Interface de GWCON (Talk 5)

La interfaz de red X.25 soporta el mandato **activate interface** de GWCON (Talk 5) con las consideraciones siguientes:

- Sólo se soporta el circuito de marcación de canal D RDSI para X.25.
- No puede activar un circuito de marcación X.25 si aún no se ha activado la red base.

El mandato **activate interface** de GWCON (Talk 5) soporta todos los mandatos específicos de interfaz de red X.25.

Reset Interface de GWCON (Talk 5)

La interfaz de red X.25 soporta el mandato **reset interface** de GWCON (Talk 5) con las consideraciones siguientes:

- Un circuito de marcación X.25 no se puede restablecer si se ha cambiado algunos de los parámetros del circuito de marcación que se configuran en el indicador Dial Circuit config (sólo se aplica a X.31 para X.25).
- No puede restablecerse una interfaz X.25 cuyo tamaño de MTU sea superior a su valor de arranque original.
- No puede restablecerse una interfaz X.25 que tenga una configuración XTP modificada y que se utilice XTP en esa interfaz.

Todos los cambios en la configuración de la interfaz de red X.25 se activan automáticamente excepto el siguiente:

Mandatos cuyos cambios no se activan por el mandato reset interface de GWCON (Talk 5)
--

CONFIG, net, set mtu

Nota: El usuario no puede incrementar el tamaño de mtu.
--

Capítulo 39. Utilización de XTP

Este capítulo describe el X.25 Transport Protocol (XTP) para transportar tráfico X.25 a través de TCP/IP. Se incluyen las secciones siguientes:

- “El X.25 Transport Protocol”
- “Comodines de dirección DTE” en la página 508
- “Función de similar de reserva XTP” en la página 508
- “XTP local” en la página 509
- “XTP y grupos de usuarios cerrados” en la página 509
- “Configuración de XTP” en la página 510
- “Procedimientos de configuración” en la página 510

El X.25 Transport Protocol

X.25 Transport Protocol (XTP) proporciona los servicios de un “reenviador de protocolos.” Un reenviador de protocolos es el punto focal para el proceso de paquetes de protocolo de entrada y salida. Los reenviadores reciben los paquetes en una interfaz de red y los envían a otra interfaz.

XTP está diseñado para funcionar con dispositivos X.25 que están situados en múltiples sitios remotos. En tales entornos, XTP puede eliminar la utilización de redes de paquetes conmutados X.25 para comunicarse con servidores de una o varias ubicaciones centralizadas.

Para hacerlo, se utilizan los direccionadores en el servidor y en las ubicaciones remotas para encapsular los datos y entregar los paquetes X.25 entre los clientes y el servidor mediante TCP/IP.

La Figura 36 en la página 506 ilustra una configuración de red antes y después de utilizar XTP.

Utilización de XTP

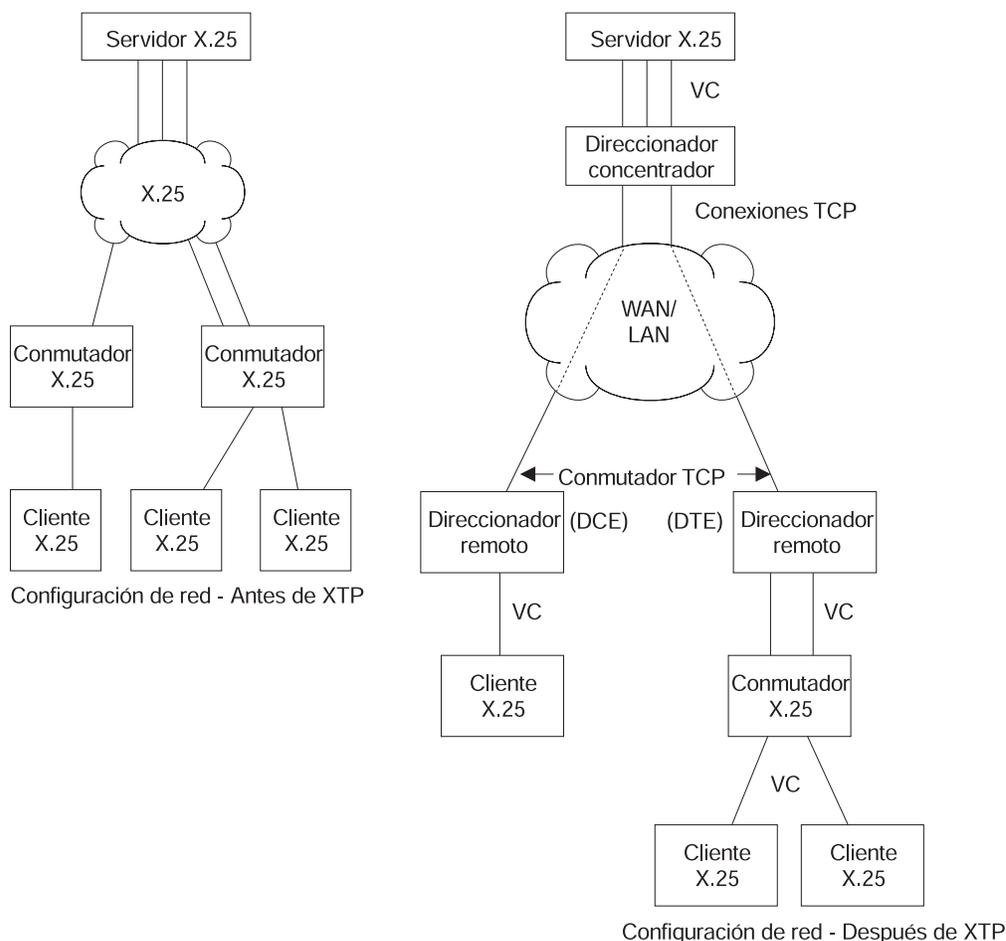


Figura 36. Configuración antes y después de XTP

Información de configuración

X.25 reconoce una llamada de entrada para XTP basándose en las direcciones de nodos configuradas para XTP. Por lo tanto, para transportar el tráfico X.25 entre los nodos X.25, debe configurar X.25 para que se correlacione con la dirección del equipo de terminal de datos (DTE) y las direcciones IP de los direccionadores con los que están conectados los nodos.

Por ejemplo, en la Figura 36, se configuran clientes X.25 en direccionadores remotos y en el direccionador concentrador. Los *direccionadores remotos* de este ejemplo son los direccionadores que conectan los clientes X.25 con la red TCP/IP que se utiliza para acceder al servidor X.25; el *direccionador concentrador* conecta el servidor X.25 con la red TCP/IP que se utiliza para acceder a los direccionadores remotos.

Nota: Al configurar XTP, si un direccionador está conectado a un conmutador X.25, se considera un DTE. Si no está conectado a ningún conmutador, se considera un DCE (Equipo de terminación de circuito de datos).

Para configurar un direccionador para XTP, defina la información siguiente en el indicador XTP `config>` y después reinicie el direccionador:

- DTE locales

- Direccionadores similares
- DTE remotos
- PVC
- CUG

DTE locales

Los nodos X.25 conectados a las interfaces X.25 del direccionador

Para configurar los DTE locales, utilice la dirección X.121 que está asignada al DTE local. Se pueden configurar múltiples DTE locales en una interfaz.

Direccionadores similares

Los direccionadores con los que el usuario se comunica mediante TCP/IP

Los direccionadores similares pueden diferir dependiendo del “punto de vista”. Por ejemplo, en la Figura 36 en la página 506, los *dos direccionadores remotos* son los direccionadores similares desde la perspectiva del direccionador concentrador. Sin embargo, el *direccionador concentrador* es el direccionador similar desde la perspectiva de los dos direccionadores remotos.

El direccionador similar se designa por su dirección IP interna.

DTE remotos

Los nodos X.25 remotos con los que los nodos X.25 locales abren conexiones e intercambian datos. Utilice la dirección X.121 que está asignada al DTE remoto.

Configure una dirección IP *exclusiva* para cada direccionador similar. Por ejemplo, en la Figura 36 en la página 506, el direccionador concentrador debe conocer la dirección IP exclusiva de cada direccionador remoto y cada direccionador remoto debe conocer la dirección IP del direccionador concentrador.

PVC Un canal permanente que permanece conectado después de que se reinicie X.25.

Los PVC, como son canales constantes, son similares a líneas telefónicas alquiladas. Un PVC, en el contexto XTP, es un PVC de un nodo DTE X.25 local para un DTE X.25 remoto.

Cuando configure un direccionador para los PVC, correlacione la dirección IP del direccionador similar y el número de PVC del DTE remoto y local. Un PVC se identifica por cuatro fragmentos de información que son:

- Los números de canal lógico de los PVC locales
- La dirección X.121 del DTE local
- Los números de canal lógico de los PVC del direccionador remoto (similar)
- La dirección X.121 del DTE remoto

CUGS Los grupos de usuarios cerrados para el protocolo XTP. Consulte la sección “Comprensión de los grupos de usuarios cerrados” en la página 465.

Se puede encontrar información de configuración adicional en las secciones “Configuración de XTP” en la página 510 y “Mandatos de configuración XTP” en la página 519.

Comodines de dirección DTE

Se dispone del comodín "*" para la configuración de direcciones DTE. Esto es además del carácter "?" que puede especificarse en una dirección DTE para representar cualquier dígito en esa posición de la dirección. Por ejemplo, una especificación de "1?2?3" puede coincidir con la dirección 18243 donde el primer, tercer y quinto dígito son 1, 2 y 3, respectivamente.

El carácter comodín "*" puede representar cualquier serie de cero o más dígitos. Se limita su utilización al final de una especificación de dirección DTE. Por ejemplo: "123*", "5555*", "9*" o "*". El caso especial de una dirección DTE "*" representa cualquier dirección DTE, incluso una dirección nula. La dirección nula es útil para manejar llamadas de entrada sin dirección de llamada en el paquete de Petición de llamada X.25.

La utilización del comodín "*" aumenta las posibilidades de añadir una dirección DTE local o remota que entre en conflicto con una dirección existente. Los mandatos **add local-dte** y **add remote-dte** se amplían para proporcionar la dirección en conflicto, cuando el usuario intenta añadir una dirección DTE que entra en conflicto con una dirección existente.

Ejemplo: xtp config> **add local-dte**

```
Interface number [0]? 1
DTE address [ ] 123456
DTE address [ ]?
```

```
XTP config>add local-dte
```

```
Interface number [0]?1
DTE address [ ]?1*
DTE address conflicts with existing DTE address 123456
```

Función de similar de reserva XTP

La función de similar de reserva permite la asociación de múltiples direccionadores similares con un DTE remoto. El usuario especifica una lista de direccionadores similares asociados con un DTE remoto.

Ejemplo:

```
XTP config>add rem
DTE address [ ]?123456
Peer router's internal IP Address [0.0.0.0]?10.0.0.2
Peer router's internal IP Address [0.0.0.0]?10.0.0.4
Peer router's internal IP Address [0.0.0.0]?11.0.0.1
Peer router's internal IP Address [0.0.0.0]?
```

Cuando se recibe una llamada de entrada para el DTE remoto, se intenta una conexión a través de cada direccionador de la lista en el mismo orden en que aparecen para el DTE remoto.

Búsqueda de un DTE remoto

Cuando un DTE inicia una llamada para un DTE remoto, se inspeccionan las dos direcciones DTE para determinar si se pueden aceptar para el transporte X.25. Si se pueden aceptar, el reenviador del protocolo X.25 Transport determina a través de qué direccionador similar se ha de intentar completar la llamada. Empieza por el primer direccionador de la lista de direccionadores similares del DTE remoto en su búsqueda. La primera condición que debe cumplirse es que debe haber una conexión TCP activa con el direccionador similar. Si no hay ninguna conexión TCP activa con el similar, se comprueba el siguiente direccionador de la lista. Cuando se

encuentra una conexión TCP activa, se intenta completar la llamada. Se inicia el Temporizador de petición de conexión para controlar el proceso de conexión de la llamada.

La búsqueda del DTE remoto termina por uno de los sucesos siguientes:

- La realización satisfactoria de la llamada a través del direccionador similar
Esto completa el proceso de establecimiento de llamada y finaliza la búsqueda del DTE remoto.
- El rechazo de la llamada por el direccionador similar
Esto hace que la búsqueda del DTE remoto prosiga en el siguiente direccionador de la lista de direccionadores similares.
- La caducidad del Temporizador de petición de conexión
Esto hace que la búsqueda del DTE remoto prosiga en el siguiente direccionador de la lista de direccionadores similares.

Si se completa un paso a través de la lista de direccionadores similares sin ninguna conexión satisfactoria a través de ninguno de los direccionadores similares, se borra la llamada para el DTE local.

Temporizador de petición de conexión

El Temporizador de petición de conexión se utiliza para asegurar que ningún procedimiento de establecimiento de llamada se quede en suspenso durante un tiempo indeterminado. Se ha configurado un temporizador para cada direccionador similar.

Ejemplo:

```
XTP config>add peer-router
Router's internal IP Address [0.0.0.0]?10.0.0.2
Connection setup timeout [230]?60
```

El Temporizador de petición de conexión puede configurarse de 10 a 480 segundos. El valor por omisión es 230 segundos. Este valor por omisión se ha determinado basándose en el hecho de que el valor por omisión para el Temporizador de petición de llamada X.25 es de 200 segundos.

El temporizador se inicia cuando se realiza un intento de completar una llamada a través de un direccionador similar. Se detiene cuando el direccionador similar acepta o rechaza el intento de llamada.

XTP local

El XTP local le permite direccionar el tráfico X.25 de entrada a la misma interfaz o a interfaces diferentes del direccionador actual. Para configurar el XTP local especifique la dirección IP interna del direccionador como una dirección de similar en el mandato **add peer**.

XTP y grupos de usuarios cerrados

XTP soporta los grupos de usuarios cerrados mediante la dirección DTE local definida por los mandatos **add local** o **add cug**. Para permitir que XTP utilice los grupos de usuarios cerrados, debe:

- Habilitar CUG o BI-CUG en las interfaces X.25 adecuadas.

Utilización de XTP

- Suministrar los CUG específicos de protocolo XTP utilizando los mandatos **add cug** y **add bi-cug**, si lo desea.
- Suministrar los números adecuados de grupos de usuarios cerrados en el mandato **add local**. Estos incluyen:
 - El número de grupos de usuarios cerrados
 - El número del grupo de usuarios cerrado preferido
 - El número de grupos de usuarios cerrados bilaterales
 - El número del grupo de usuarios cerrado bilateral preferido
- Habilitar la inserción o supresión de CUG para la interfaz en los mandatos **national enable cug_insertion** o **national enable cug_deletion**, si lo desea.
- Habilitar la opción de alteración temporal de CUG 0 en el mandato **national enable cug 0 override**, si lo desea.

Configuración de XTP

XTP es un reenviador de protocolo utilizado para transportar tráfico X.25 mediante TCP/IP. XTP permite que los dispositivos X.25 existentes se comuniquen a través de la red troncal TCP/IP y se migren de una red X.25 a otra red de su elección.

Procedimientos de configuración

Esta sección define los detalles para configurar la red visualizada en la Figura 37 en la página 511.

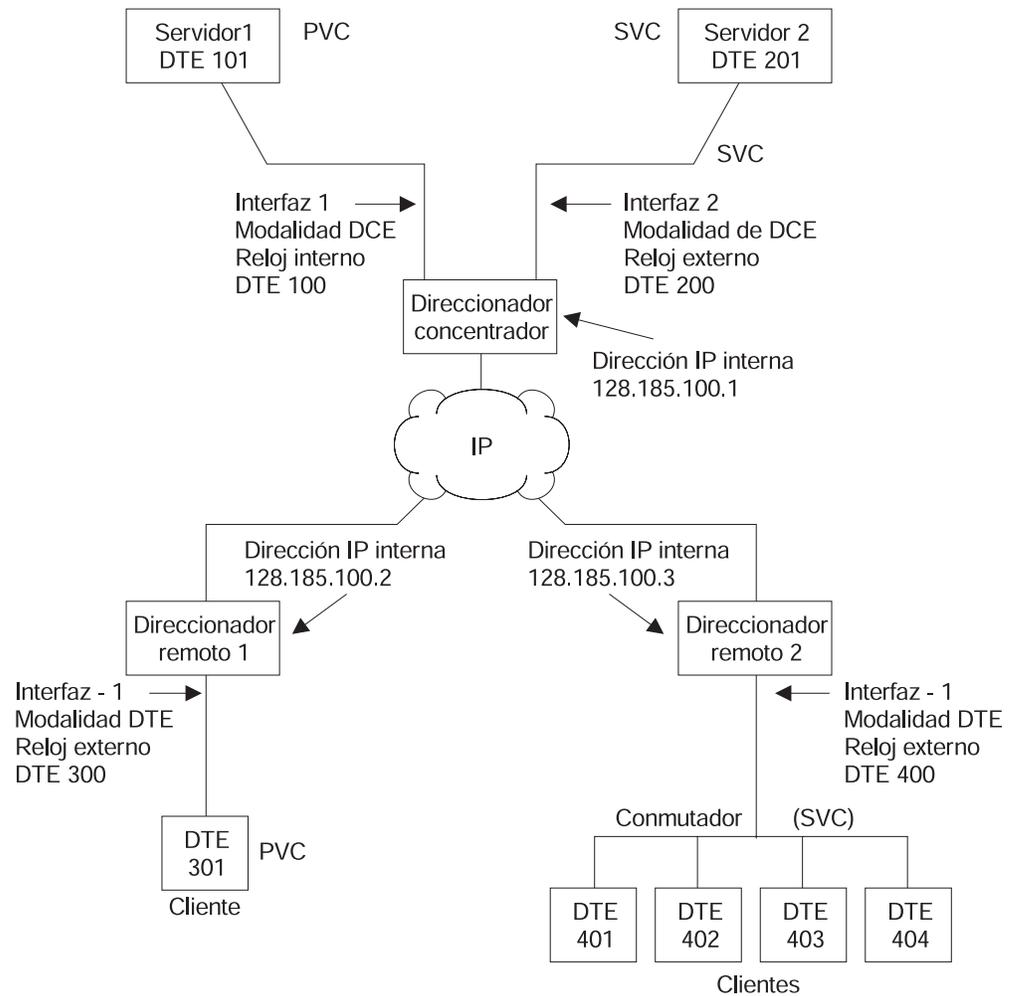


Figura 37. Ejemplo de configuración XTP

Esta configuración muestra tres direccionadores, el direccionador concentrador, el Direccionador remoto 1 y el Direccionador remoto 2. Para que XTP sea operativo en esta red, lleve a cabo los pasos siguientes para cada uno de estos direccionadores:

- Establezca el enlace de datos
- Configure la interfaz IP
- Configure X.25
- Establezca los valores de Personalidad nacional
- Defina la dirección IP
- Establezca la dirección IP interna
- Configure XTP

Nota: Las nuevas configuraciones no surten efecto hasta que se reinicia el direccionador.

Establecimiento del enlace de datos

El enlace de datos define el protocolo que está utilizando para enviar paquetes de datos a través de la red. Defina el enlace de datos entre el direccionador que está configurando y cada interfaz serie. El ejemplo de la Figura 37 configura un direccionador concentrador con tres interfaces serie, dos para X.25 y una para PPP.

Utilización de XTP

Establezca el protocolo de enlace de datos para las interfaces serie:

```
Config>set data-link X25 1
Config>set data-link x25 2
Config>set data-link ppp 3
```

Configuración de la interfaz IP

En la Figura 37 en la página 511, la interfaz IP es PPP; entre **network 3** en el indicador Config> para configurar esta interfaz PPP:

```
Config>network 3
PPP interface configuration
```

Nota: Este procedimiento no incluye los detalles acerca de la configuración de PPP. Para ver los detalles, consulte la publicación *Guía del usuario de software*

Configuración de X.25

Antes de configurar XTP, configure los parámetros X.25 para cada interfaz. El ejemplo siguiente configura los parámetros básicos para X.25 y está basado en la topología de la Figura 37 en la página 511.

Los parámetros que necesita configurar dependen de la topología de la red. Para obtener detalles acerca de todos los parámetros X.25, consulte la publicación *Guía del usuario de software*

Interfaz 1

Utilice las instrucciones siguientes para configurar la *Interfaz 1* del direccionador concentrador, tal como se define en la Figura 37 en la página 511.

1. En el indicador Config>, entre **network** seguido del número de la interfaz X.25. En este ejemplo, es la interfaz 1.

```
Config>network 1
X.25 User Configuration
X.25 Config>
```

2. Añada el protocolo XTP a la interfaz X.25 y defina los valores generales de la interfaz. Entre **add protocol xtp** en el indicador X.25 Config>. Sólo es necesario entrar este mandato *una vez*.

```
X.25 Config>add protocol xtp
Window Size [2]?
Default Packet Size [128]?
Maximum Packet Size [256]?
```

3. Especifique la dirección de la red entrando **set address** dirección de nodo X.25. En la Figura 37 en la página 511, la dirección de nodo (dirección DTE) es 100.

```
X.25 Config>set address 100
```

4. Entre **set clocking** seguido de **internal** o **external** basándose en el tipo de direccionador.

```
X.25 Config>set clocking internal
```

5. Entre **set speed** seguido por la velocidad de acceso (velocidad de línea).

```
X.25 Config>set speed
Access rate in bps [9600]?19200
```

6. Entre **set equipment-type** y especifique si los niveles de trama y de paquete actúan como DCE o DTE.

```
X.25 Config>set equipment-type dce
```

7. Entre **set pvc** y defina el PVC inferior y superior que está utilizando.

```
X.25 Config>set pvc low 1
X.25 Config>set pvc high 1
```

8. Entre **add pvc** para definir PVC individuales.

```
X.25 Config>add pvc
Protocol [IP]?xtp
Packet Channel [1]?
Destination X.25 Address [ ]?101
Window Size [2]?
Packet Size [128]
```

9. (Opcional) Entre **national enable truncate-called-addresses**. Si desea truncar el tamaño de la dirección llamada, entre **national set truncate-called-addr-size** seguido por el número de dígitos al que se ha de truncar la dirección DTE llamada.
10. (Opcional) Habilite el soporte de CUG, la inserción de CUG y la supresión de CUG, según proceda.

Interfaz 2

Utilice las instrucciones siguientes para configurar la interfaz 2.

1. En el indicador Config>, entre **network** seguido del número de la interfaz X.25. En la Figura 37 en la página 511, es 2.

```
Config>network 2
X.25 User Configuration
X.25 Config>
```

2. Utilice los mismos procedimientos que los definidos en la sección “Interfaz 1” en la página 512 para establecer los siguientes parámetros de la interfaz 2:
 - dirección = 200
 - cronometraje = internal
 - velocidad = 19200
 - equipo = dce
3. Entre **set svc** y defina el SVC inferior y superior que está utilizando.

Hay tres tipos de SVC: bidireccional, de entrada y de salida. Los valores por omisión son “svc low-two-way = 1” y “svc high-two-way = 64.” Todos los demás tipos de SVC toman por omisión 0. Para obtener información adicional sobre SVC y PVC, consulte la publicación *Guía del usuario de software*

```
X.25 Config>set svc ?
X.25 Config>set svc low-inbound 0
X.25 Config>set svc high-inbound 0
X.25 Config>set svc low-outbound 0
X.25 Config>set svc high-outbound 0
X.25 Config>set svc low-two-way 2
X.25 Config>set svc high-two-way 2
```

4. Salga del indicador X.25 Config>.

```
X25 Config>exit
Config>
```

Establecimiento de la personalidad nacional

Cada red pública X.25 tiene su propia configuración estándar. La Personalidad nacional hace referencia a un grupo de 28 variables que definen las características de la red de datos pública. Estas variables proporcionan información de control al direccionador para los paquetes transferidos a través del enlace e influyen en los recursos X.25 utilizados entre el direccionador XTP y su DTE local.

Todos los recursos contenidos en las peticiones de llamada de entrada se pasan al direccionador similar, sin tener en cuenta si se ha configurado el direccionador local para soportar este recurso. Por ejemplo, cuando se pide la negociación del tamaño de paquete en la llamada de entrada y la negociación de control de flujo no está configurada en el direccionador.

El direccionador asegurará que cualquier tamaño de paquete y tamaño de ventana que se negocie esté dentro del rango especificado al definir la interfaz X.25. Por ejemplo, una ventana de paquete mayor que 7 se negocia a la baja hasta 7, si no se ha definido packet-ext-seq-mode para la interfaz X.25.

Utilización de XTP

Para ver los valores de configuración, entre **list detailed** en el indicador X.25 Config>. Para establecer los valores por omisión para la personalidad nacional, entre **set national-personality** en el indicador X.25 Config>. Para obtener más información, consulte la publicación *Guía del usuario de software*

Definición de la dirección IP

Antes de configurar el direccionador concentrador (tal como se ve en la Figura 37 en la página 511) para XTP, defina la dirección IP para este direccionador. Entre **protocol ip** en el indicador Config> y entre **add address** en el indicador IP config>.

```
Config>protocol ip
IP config>add address
Which net is this address for [0]?3
New address [0.0.0.0]?128.185.100.7
Address mask [255.255.0.0]?255.255.255.0
```

Establecimiento de la dirección IP interna

Cada direccionador identifica sus direccionadores similares mediante la dirección IP interna de los direccionadores similares.

Para establecer la dirección IP interna del direccionador similar, entre **set internal IP address** en el indicador IP Config>.

```
IP config>set internal-ip-address
Internal IP address [0.0.0.0]?128.185.100.1
```

Configuración de XTP

Después de haber configurado X.25 y definido la dirección IP, está preparado para configurar XTP para el direccionador.

Si necesita más información de configuración al configurar XTP, consulte la sección “Mandatos de configuración XTP” en la página 519.

Nota: Cuando configure la red para XTP, recuerde que los direccionadores similares son siempre los direccionadores con los que se comunica a través de TCP/IP. Por lo tanto, el direccionador similar puede diferir dependiendo del punto de vista. Al configurar los direccionadores definidos como Direccionador remoto 1 y Direccionador remoto 2 en la Figura 37 en la página 511, para ellos el direccionador similar es el direccionador concentrador.

Realice los pasos siguientes para configurar XTP para el direccionador:

1. Para acceder al indicador XTP config>, entre **protocol xtp** en el indicador Config>.
2. Añada la interfaz 1 a la configuración XTP. Entre **add local-dte** en el indicador XTP Config>.

```
XTP config>add local-dte
Interface number [0]?1
Allow inbound calls without calling DTE address? (Y or N) [N]? n
DTE address [ ]?101
Pref CUG [ ]? 18
CUG (2) [ ]? 2
CUG (3) [ ]?
Pref BI-CUG [0]?
DTE address [ ]?
```

Si se entra una dirección DTE nula se finaliza la entrada del mandato.

3. Añada la interfaz 2 a la configuración XTP. Entre **add local-dte** en el indicador XTP Config>.

```
XTP config>add local-dte
Interface number [0]?2
Allow inbound calls without calling DTE address? (Y or N) [N]? n
DTE address [ ]?201
DTE address [ ]?
```

Si se entra una dirección DTE nula se finaliza la entrada del mandato.

4. (Opcional) Añada los CUG específicos de protocolo XTP.

```
add cug
Pref CUG [ ]? 11
CUG (2) [ ]? 12
CUG (3) [ ]? 13
CUG (4) [ ]? 14
CUG (5) [ ]? 15

add bi-cug
Pref BI-CUG [ ]? 21
BI-CUG (2) [ ]? 22
BI-CUG (3) [ ]?
```

5. Añada el Direccionador remoto 1 como direccionador similar. Entre **add peer-router** y entre la dirección IP de este direccionador.

```
XTP config>add peer-router
Router's internal IP Address [0.0.0.0]?128.185.100.2
Connection setup timeout [230]?
```

6. Añada el DTE remoto para el Direccionador remoto 1. Entre **add remote-dte** y entre las direcciones IP y DTE para este DTE.

```
XTP config>add remote-dte
DTE address [ ]?301
Peer router's internal IP Address [0.0.0.0]?128.185.100.2
Peer router's internal IP Address [0.0.0.0]?
```

Nota: Un DTE remoto sólo es *necesario* si se aplica una de las situaciones siguientes:

- El Direccionador concentrador iniciará conexiones XTP con el DTE remoto debido a llamadas de entrada de sus DTE locales.
- El DTE forma parte de una definición de PVC XTP.

7. Añada el Direccionador remoto 2 (como direccionador similar). Entre **add peer-router** y entre la dirección IP de este direccionador.

```
XTP config>add peer-router
Router's internal IP Address [0.0.0.0]?128.185.100.3
Connection setup timeout [230]?
```

8. Añada los DTE remotos para el Direccionador remoto 2. Entre **add remote-dte** y entre las direcciones IP y de DTE para este DTE.

```
XTP config>add remote-dte
DTE address [ ]?401
Peer router's internal IP Address [0.0.0.0]?128.185.100.3
Peer router's internal IP Address [0.0.0.0]?
```

```
XTP config>add remote-dte
DTE address [ ]?402
Peer router's internal IP Address [0.0.0.0]?128.185.100.3
Peer router's internal IP Address [0.0.0.0]?
```

```
XTP config>add remote-dte
DTE address [ ]?403
Peer router's internal IP Address [0.0.0.0]?128.185.100.3
Peer router's internal IP Address [0.0.0.0]?
```

```
XTP config>add remote-dte
DTE address [ ]?404
Peer router's internal IP Address [0.0.0.0]?128.185.100.3
Peer router's internal IP Address [0.0.0.0]?
```

9. Añada un PVC XTP para asociar lógicamente el PVC local con el Servidor 1 que tiene el DTE remoto 301.

Utilización de XTP

```
XTP config>add pvc
Local PVC Range Start [1]?
Local PVC Range End [1]?
Local X.25 DTE address [ ]? 101
Remote PVC Range Start [1]?
Remote PVC Range End [1]?
Remote X.25 DTE address [ ]?301
```

Cuando entre las direcciones DTE, puede especificar cualquiera de los siguientes:

Un '?' en lugar de cualquier dígito. El '?' significa un solo dígito cualquiera en esta posición de dígito.

Un '*' como el último dígito de una dirección para representar cualquier combinación de cero o más dígitos.

Ejemplo de configuración de direccionadores remotos

El siguiente es un ejemplo de configuración de Direccionador remoto 1 y Direccionador remoto 2 (consulte la Figura 37 en la página 511). El proceso es igual al descrito en la sección "Procedimientos de configuración" en la página 510.

Direccionador remoto 1

```
*talk 6

Config>set data-link x25 1
Config>set data-link ppp 2
Config>network 1

X.25 Config>set address 300
X.25 Config>set clocking internal
X.25 Config>set speed 19200
X.25 Config>set equipment-type dce
X.25 Config>set pvc low 1
X.25 Config>set pvc high 1
X.25 Config>add pvc
Protocol [IP]?xtp
Packet Channel [1]?1
Destination X.25 Address [ ]?301

Window Size [2]?
Packet Size [128]?
X.25 Config>exit
Config>

Config>protocol ip
IP config>add address
Which net is this address for [0]?2
New address [0.0.0.0]?128.185.100.8
Address mask [255.255.0.0]?255.255.255.0

IP config>set internal-ip-address
Internal IP address [0.0.0.0]?128.185.100.2
IP Config>exit
Config>

Config>protocol xtp
XTP config>add local-dte
Interface number [0]?1
Allow inbound calls without calling DTE address? (Y or N) [N]? n
DTE address [ ]?301
DTE address [ ]?

XTP config>add peer-router
Router's IP address?128.185.100.1

XTP config>add remote-dte
DTE address [ ]?101
Peer router's internal IP Address [0.0.0.0]?128.185.100.1
Peer router's internal IP Address [0.0.0.0]?

XTP config>add pvc
Local PVC Range Start [1]?
Local PVC Range End [1]?
Local X.25 DTE address [ ]? 101
```

```

Remote PVC Range Start [1]?
Remote PVC Range End [1]?
Remote X.25 DTE address [ ]? 301

```

Direccionador remoto 2

```
*talk 6
```

```

Config>set data-link x25 1
Config>set data-link ppp 2
Config>network 1

```

```

X.25 Config>set address 400
X.25 Config>set clocking external
X.25 Config>set speed 19200
X.25 Config>set equipment-type dte
X.25 Config>set svc low-inbound 0
X.25 Config>set svc high-inbound 0
X.25 Config>set svc low-outbound 0
X.25 Config>set svc high-outbound 0
X.25 Config>set svc low-two-way 1
X.25 Config>set svc high-two-way 64
X.25 Config>add protocol
Protocol [IP]?xtp
Window Size [2]?
Default Packet Size [128]?
Maximum Packet Size [256]?
X.25 Config>exit

```

```

Config>protocol ip
IP config>add address
Which net is this address for [0]?2
New address [0.0.0.0]?128.185.100.9
Address mask [255.255.0.0]?255.255.255.0

```

```

IP config>set internal-ip-address
Internal IP address [0.0.0.0]?128.185.100.3
IP Config>exit
Config>

```

```

Config>protocol xtp
XTP config>add local-dte
Interface number [0]?1
Allow inbound calls without calling DTE address? (Y or N) [N]? n
DTE address [ ]?401
Pref CUG [ ]? 23
CUG (2) [ ]? 24
CUG (3) [ ]? 25
CUG (4) [ ]? 26
CUG (5) [ ]? 27

DTE address [ ]?402
Pref CUG [ ]?
DTE address [ ]?403
Pref CUG [ ]?
DTE address [ ]?404
Pref CUG [ ]?
DTE address [ ]?

```

```

XTP Config>add peer-router
Router's IP address?128.185.100.1

```

```

XTP config>add remote-dte
DTE address [ ]?201
Peer router's internal IP Address [0.0.0.0]?128.185.100.1
Peer router's internal IP Address [0.0.0.0]?
XTP config>exit

```

```
Config>
```

Utilización de XTP

Capítulo 40. Configuración y supervisión de XTP

Este capítulo describe los mandatos de configuración y supervisión de XTP. Incluye las secciones siguientes:

- “Mandatos de configuración XTP”
- “Mandatos de supervisión XTP” en la página 526
- “Soporte para la reconfiguración dinámica de la interfaz de red X.25” en la página 530

Mandatos de configuración XTP

Esta sección describe los mandatos de configuración XTP.

Para acceder al entorno de configuración de XTP, entre el mandato **protocol xtp** en el indicador `Config>`.

```
Config> p xtp
XTP config>
```

Entre los mandatos de configuración XTP en el indicador `XTP config>`.

Tabla 66. Resumen de los mandatos de configuración XTP

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página 10.
Add	Añade una interfaz, un direccionador similar, grupos de usuarios cerrados, un DTE remoto o definiciones de PVC.
Change	Cambia un direccionador similar, un DTE remoto o una definición de PVC.
Delete	Suprime un DTE local, un direccionador similar, grupos de usuarios cerrados, un DTE remoto o una definición de PVC.
Enable-XTP	Activa el reenviador XTP.
Disable-XTP	Desactiva el reenviador XTP.
Set	Establece el valor del temporizador de mantener activo XTP.
List	Lista las interfaces, los direccionadores similares, los DTE remotos y las definiciones de PVC.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página 11.

Add

Añade un nodo X.25 local, un direccionador similar, un nodo X.25 remoto con los direccionadores correspondientes o un PVC desde un nodo X.25 local a un nodo X.25 remoto.

Se incluye el direccionamiento con comodín en el reenviador XTP. Cuando se entran las direcciones DTE locales o remotas, pueden contener un carácter comodín (? o *). Para obtener información adicional sobre la utilización de comodines, consulte la sección “Comodines de dirección DTE” en la página 508.

Sintaxis:

```
add                bi-cug
                   cug
                   local-dte
```

Mandatos de configuración XTP (Talk 6)

peer-router

_remote-dte

pvc

cug Especifica los números de grupos de usuarios cerrados para el protocolo XTP. El primer CUG que se le solicita es el preferido. **Valores válidos:** Del 0 al 9999

Valor por omisión: Ninguno

Ejemplo:

```
add cug
Pref CUG [ ]? 114
CUG (2) [ ]? 314
CUG (3) [ ]? 478
CUG (4) [ ]?
```

bi-cug Especifica los números de grupos de usuarios cerrados bilaterales para el protocolo XTP. El primer bi-cug que se solicita es el preferido. **Valores válidos:** Del 0 al 9999

Valor por omisión: Ninguno

Ejemplo:

```
add bi-cug
Pref BI-CUG [ ]? 50
BI-CUG (2) [ ]? 51
BI-CUG (3) [ ]? 52
BI-CUG (4) [ ]? 53
BI-CUG (5) [ ]? 54
```

local-dte

Añade direcciones de DTE X.25 o los nodos X.25, que se comunican con el direccionador de la interfaz especificada. Los números válidos de interfaces para utilizar con XTP son de 0 a 255.

Puede configurar múltiples nodos locales. Sin embargo, si se ha seleccionado la opción para permitir llamadas de entrada sin ninguna dirección de DTE de llamada y se recibe esa llamada, la *última* dirección DTE local añadida se convierte en la dirección de DTE de llamada para esa llamada.

Ejemplo:

```
add local-dte

Interface number [0]?4
Allow inbound calls without calling DTE address? (Y or N) [N]? y
DTE address [ ]?101
Pref CUG [ ]? 23
CUG (2) [ ]? 24
CUG (3) [ ]? 25
CUG (4) [ ]? 26
CUG (5) [ ]? 27
Pref BI-CUG [ ]? 6
BI-CUG (2) [ ]? 7
BI-CUG (3) [ ]? 8
BI-CUG (4) [ ]? 9
BI-CUG (5) [ ]? 10
DTE address [ ]?
```

peer-router

Añade direccionadores similares. Entre las direcciones IP internas de los direccionadores a los que están conectados los nodos X.25 remotos. Puede utilizar estas direcciones IP para abrir conexiones TCP y transportar paquetes X.25 que contienen las peticiones de conexión y los datos X.25.

Mandatos de configuración XTP (Talk 6)

Si la dirección IP interna que configura para el direccionador similar es la dirección IP interna de este direccionador, el software establece una conexión XTP local.

Ejemplo:

```
add peer-router
```

```
Router's internal IP Address [0.0.0.0]?128.185.100.2  
Connection setup timeout [230]?
```

remote-dte

Añade nodos X.25 remotos y los direccionadores correspondientes. Puede conectar nodos remotos con nodos X.25 locales para que intercambien datos. Debe configurar una dirección IP para cada nodo X.25 remoto que configure. Cualquier petición o dato enviado a este nodo remoto va al direccionador. Entonces el direccionador utiliza una de sus interfaces X.25 locales para reenviar los datos al nodo X.25.

Defina un DTE remoto si el direccionador va a iniciar conexiones XTP con el DTE remoto debido a llamadas de entrada desde sus DTE locales o si el DTE remoto forma parte de una definición de PVC XTP.

Para utilizar el XTP local, la dirección del direccionador similar debe ser la dirección interna del direccionador local y debe definirse previamente la dirección de DTE utilizando el mandato **add local**.

Ejemplo:

```
add remote-dte
```

```
DTE address [ ]?301  
Peer router's internal IP Address [0.0.0.0]?128.185.100.2  
Peer router's internal IP Address [0.0.0.0]?
```

pvc

Añade un PVC desde un nodo X.25 local a un nodo X.25 remoto.

Es necesario que existan tres elementos para activar una configuración de PVC:

- Un PVC X.25 desde el direccionador al nodo X.25 local
- Un PVC X.25 desde el direccionador similar al nodo X.25 remoto
- Una conexión TCP con el direccionador similar donde reside el nodo remoto

Ejemplo:

```
XTP config>add pvc  
Local PVC Range Start [1]?  
Local PVC Range End [1]?  
Local X.25 DTE address [ ]? 101  
Remote PVC Range Start [1]?  
Remote PVC Range End [1]?  
Remote X.25 DTE address [ ]? 301
```

Notas:

1. Cuando añada los PVC a la configuración del direccionador, también debe configurar el PVC en X.25. Para ver los detalles sobre la configuración de interfaces X.25, consulte la publicación *Guía del usuario de software*
2. Para XTP local, debe definir el PVC en ambas direcciones. Esta dirección es necesaria porque el direccionador está realizando las dos funciones, local y remota. Por ejemplo, para definir el PVC local 8 y el PVC remoto 10 cuando se utilice XTP local, debe hacer lo siguiente:

```
XTP config>add pvc  
Local PVC Range Start [1]? 8  
Local PVC Range End [1]? 8  
Local X.25 DTE address [ ]? 108
```

Mandatos de configuración XTP (Talk 6)

```
Remote PVC Range Start [1]? 10
Remote PVC Range End [1]? 10
Remote X.25 DTE address [ ]? 301

XTP config>add pvc
Local PVC Range Start [1]? 10
Local PVC Range End [1]? 10
Local X.25 DTE address [ ]? 310
Remote PVC Range Start [1]? 8
Remote PVC Range End [1]? 8
Remote X.25 DTE address [ ]? 108
```

3. Puede definirse un rango de PVC mediante los parámetros de inicio de rango de PVC y fin de rango de PVC. Debe definirse el mismo número de circuitos en el rango de PVC locales que en el rango de PVC remotos. Por ejemplo, si se define un circuito en el rango de PVC locales, debe definirse un circuito en el rango de PVC remotos.
4. Los PVC definidos deben estar en el rango de 1 a 255.

Nota: Cuando añada los PVC a la configuración del direccionador, también debe configurar el PVC en X.25. Para ver los detalles sobre la configuración de interfaces X.25, consulte la publicación *Guía del usuario de software*

Change

Cambia un direccionador similar, un DTE remoto o un PVC de la configuración XTP.

Sintaxis:

```
change peer-router
remote-dte
pvc
```

peer-router

Cambia direccionadores similares específicos de la configuración XTP.

Ejemplo:

```
change peer-router
Router IP Address [0.0.0.0]?128.185.100.2
```

remote-dte

Cambia DTE remotos específicos de la configuración XTP.

Ejemplo:

```
change remote-dte
DTE address [ ]?401
Peer router's internal IP Address [0.0.0.0]?128.185.100.2
Peer router's internal IP Address [0.0.0.0]?
```

pvc Cambia las definiciones de PVC para todos los PVC del rango definido por el parámetro Inicio de rango de PVC locales.

Ejemplo:

```
change pvc
Local PVC Range Start [1]?1
Local DTE address [ ]?301
```

Delete

Suprime un DTE local, un direccionador similar, un DTE remoto o un PVC de la configuración XTP.

Sintaxis:

```
delete          bi-cug  
                  cug  
                  local-dte  
                  peer-router  
                  remote-dte  
                  pvc
```

bi-cug Suprime un número de grupo de usuarios cerrado bilateral utilizado por esta interfaz.

Valores válidos:

Y Suprime el CUG actual.
N No suprime el CUG actual.
ALL Suprime todos los CUG restantes.
Q Detiene la supresión de cualquier CUG que quede.

Ejemplo:

```
delete bi-cug  
Delete Pref BI-CUG [Y]?  
Delete BI-CUG (2) [Y]? N  
Delete BI-CUG (3) [Y]? q
```

cug Suprime los números de grupos de usuarios cerrados que utiliza esta interfaz. Este mandato funciona de manera similar al mandato **delete bi-cug**.

Ejemplo:

```
del cug  
  
Delete Pref CUG [Y]?  
Delete CUG (2) [Y]?  
Delete CUG (3) [Y]? q
```

local-dte

Suprime interfaces locales específicas de la configuración XTP.

Ejemplo:

```
delete local-dte  
  
Interface number [0]?1  
DTE address [ ]?101  
Record deleted
```

peer-router

Suprime direccionadores similares específicos de la configuración XTP.

Ejemplo:

```
delete peer-router  
  
Router IP Address [0.0.0.0]?128.185.100.2  
Record deleted
```

remote-dte

Suprime DTE remotos específicos de la configuración XTP.

Ejemplo: delete remote-dte

```
DTE address [ ]?401
```

pvc Suprime las definiciones PVC para todos los PVC del rango definido por el parámetro de Inicio de rango de PVC locales.

Ejemplo:

Mandatos de configuración XTP (Talk 6)

```
delete pvc
Local PVC Range Start [1]?1
Local DTE address [ ]?301
Record deleted
```

Enable

Activa el reenviador XTP.

Sintaxis: enable-xtp

Ejemplo: enable-xtp

Disable

Desactiva el reenviador XTP.

Sintaxis: disable-xtp

Ejemplo: disable-xtp

Set

Establece el Temporizador de mantener activo XTP.

Sintaxis: keep-alive-timer

Ejemplo:

```
set keep-alive-timer
```

```
Keepalive timer in seconds [10]?60
```

List

Lista las interfaces, los direccionadores similares, los DTE remotos o los PVC.

Sintaxis:

```
list          all
              cugs
              keep-alive-timer
              local-dtes
              peer-routers
              remote-dtes
              pvcs
              xtp-status
```

all Visualiza todas las interfaces, los direccionadores similares, los DTE remotos y los PVC configurados para XTP.

Ejemplo:

```
list all
```

```
STATUS: XTP-DISABLED
```

```
Local DTEs:
```

```
Interface      DTE Address
1              44444      Calling DTE address is optional
Pref CUG      : 7777 Others : 9999 0
```

Mandatos de configuración XTP (Talk 6)

```
Pref BI-CUG : 0   Others :  
4           33333 Calling DTE address is optional  
Pref CUG    : 1   Others : 2 3 4 5  
Pref BI-CUG : 6   Others : 7 8 9 10
```

Peer Routers Connection Timeout

```
Remote DTEs:  
DTE Address Peer Router(s)  
  
PVCs:  
Local PVC Local DTE Remote PVC Remote DTE  
LCN Range Address LCN Range Address  
  
Pref CUG : 114 Others : 314 478  
Pref BI-CUG : 1 Others : 1 1 1 1111
```

KEEP-ALIVE-TIMER: 10 seconds

cugs Lista los números de CUG y BI-CUG definidos para el protocolo XTP.

keep-alive-timer

Visualiza todo el tiempo de mantener activo configurado para XTP.

local-dtes

Visualiza todos los DTE locales configurados para XTP.

Ejemplo:

```
list local-dtes
```

```
Local DTEs:  
Interface DTE Addr  
1         101 Calling DTE address is required  
2         201 Calling DTE address is required
```

peer-routers

Visualiza todos los direccionadores similares configurados para XTP.

Ejemplo:

```
list peer-routers
```

```
Peer Routers:  
128.185.100.2  
128.185.100.3
```

pvcs Visualiza todos los PVC configurados para XTP.

Ejemplo-

```
list pvc
```

```
PVCs:  
  
Local PVC Local DTE Remote PVC Remote DTE  
LCN Range Address LCN Range Address  
1 - 1     100     1 - 1     301
```

remote-dtes

Visualiza todos los DTE remotos configurados para XTP.

Ejemplo:

```
list remote-dtes
```

```
Remote DTEs:  
DTE Address Peer Router  
301         128.185.100.2  
401         128.185.100.3  
402         128.185.100.3  
403         128.185.100.3  
404         128.185.100.3
```

xtp-status

Visualiza el estado de XTP que indica si está habilitado o inhabilitado.

Ejemplo:

Mandatos de configuración XTP (Talk 6)

```
list xtp-status
STATUS: XTP-ENABLED
```

Mandatos de supervisión XTP

Esta sección describe los mandatos de supervisión XTP. Estos mandatos le permiten visualizar las interfaces activas actualmente, los direccionadores similares, el DTE remoto, los PVC y los SVC. También le permiten añadir o suprimir dinámicamente interfaces, DTE o direccionadores similares.

Para visualizar el indicador XTP>, entre **protocol xtp** en el indicador de supervisión (+):

```
+protocol xtp
X.25 Transport Console
XTP>
```

Entre los mandatos de supervisión XTP en el indicador XTP>.

Tabla 67. Resumen de los mandatos de supervisión XTP

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado "Cómo obtener ayuda" en la página 10.
Add	Añade dinámicamente DTE locales, DTE remotos o direccionadores similares
Delete	Suprime dinámicamente configuraciones para DTE locales, DTE remotos o direccionadores similares
List	Visualiza estadísticas de PVC o SVC individuales e información general
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página 11.

Add

Añade una interfaz, un direccionador similar o un DTE remoto a la configuración XTP.

Sintaxis:

```
add                local-dtes
                    peer-router
                    remote-dtes
```

local-dtes

Añade una interfaz local a la configuración XTP.

Ejemplo:

```
add local-dtes

Interface number [0]?1
DTE address [ ]?101
```

peer-router

Añade un direccionador similar a la configuración XTP.

Ejemplo:

```
add peer-router

Router's IP Address [0.0.0.0]?128.185.100.2
```

remote-dtes

Añade un DTE remoto a la configuración XTP.

Ejemplo:

```
add remote-dtes
Peer router's IP Address [0.0.0.0]?128.185.100.2
DTE address [ ]?301
DTE address [ ]?
```

Delete

Suprime un DTE local, un direccionador similar o un DTE remoto de la configuración de direccionador.

Sintaxis:

```
delete                _local-dtes
                        _peer-router
                        _remote-dtes
```

local-dtes

Suprime una interfaz local de la configuración XTP.

Ejemplo:

```
delete local-dtes
Interface Number [0]?1
DTE address [ ]?101
DTE address [ ]?
```

peer-router

Suprime un direccionador similar de la configuración XTP.

Ejemplo: delete peer-router

```
Router's IP Address [0.0.0.0]?123.185.100.2
```

remote-dtes

Suprime un DTE remoto de la configuración XTP.

Ejemplo:

```
delete remote-dtes
DTE address [ ]?401
DTE address [ ]?
```

List

Visualiza las interfaces activas actuales, los direccionadores similares, los DTE remotos, los PVC y los SVC.

Sintaxis:

```
list                _all
                        _xtp-status
                        _local-dtes
                        _peer-routers
                        _remote-dtes
                        _pvcs
                        _pvc-detailed
                        _pvcs-all-detailed
```

Mandatos de supervisión XTP (Talk 5)

svcs

svc-detailed

svc-all-detailed

all Visualiza la salida de todas las opciones del mandato list.

Ejemplo:

list all

STATUS: XTP-ENABLED
KEEP-ALIVE TIMER = 20 seconds

LIST OF LOCAL DTES

```
-----  
Interface      Local  
  No          DTE  
  1           101      Calling DTE address is required  
  2           201      Calling DTE address is required
```

LIST OF PEER ROUTERS

```
-----  
Router          CNN      Number      Received      Sent  
                State    of Ckts      Pkts  Bytes      Pkts  Bytes  
128.185.100.3   Active   15          60   1533       12   142  
128.185.100.2   Active   12          63   1620       10   130
```

LIST OF REMOTE DTES

```
-----  
Remote          Router  
DTE             IP  
404             128.185.100.3  
403             128.185.100.3  
402             128.185.100.3  
401             128.185.100.3  
301             128.185.100.2
```

LIST OF PVCs

```
-----  
Index   Int   PVC   Local   Local   Remote   Remote  
No      No   State LCN     DTE     LCN     DTE  
  1     1   Active 100     100     301
```

LIST OF SVCS (list svcs)

```
-----  
Index   Int   Logical   SVC   Local   Remote   Peer  
No      No   Channel   State DTE     DTE     Router  
  1     2     5         ACT   333333333333 4444444444444 3.3.3.3
```

SVC 1 IN DETAIL (list svc-detailed)

```
-----  
Int   Log   SVC   Received      Sent      Dropped  
No   Chn  State  Pkts  Bytes  Pkts  Bytes  Pkts  Bytes  
  2   5   ACT     2   116     2   106     0     0
```

LIST OF SVCS (svcs-all-detailed)

```
-----  
Int   Log   SVC   Received      Sent      Dropped  
No   Chn  State  Pkts  Bytes  Pkts  Bytes  Pkts  Bytes  
  2   5   ACT     1     7     1     2     0     0
```

xtp-status

Visualiza si XTP está habilitado/inhabilitado y el tiempo especificado para el Temporizador de mantener activo.

Ejemplo:

list xtp-status

STATUS: XTP-ENABLED
KEEP-ALIVE-TIMER = 20 seconds

local-dtes

Visualiza todas las interfaces configuradas para XTP.

Ejemplo:

`list local-dtes`

```
LIST OF LOCAL DTES
-----
Interface      Local
No             DTE
1              101   Calling DTE address is required
2              201   Calling DTE address is required
```

peer-routers

Visualiza todos los direccionadores similares configurados para XTP.

Ejemplo:

`list peer-routers`

```
LIST OF PEER ROUTERS
-----
Router          CNN      Number      Received      Sent
                State    of Ckts      Pkts  Bytes      Pkts  Bytes
128.185.100.3   Active   15           60   1533        12   142
128.185.100.2   Active   12           63   1620        10   130
```

remote-dtes

Visualiza todas las interfaces remotas configuradas para XTP.

Ejemplo:

`list remote-dtes`

```
LIST OF REMOTE DTES
-----
Remote      Router
DTE         IP
404         128.185.100.3
403         128.185.100.3
402         128.185.100.3
401         128.185.100.3
301         128.185.100.2
```

pvc Visualiza todos los PVC configurados para XTP.

Ejemplo:

`list pvcs`

```
LIST OF PVCS
-----
Index  Int  PVC  Local  Local  Remote  Remote
No     No  State LCN    DET    LCN     DTE
1      1   Active 100    100    LCN     301
```

pvc-detailed

Visualiza información detallada para una definición de PVC específica. Para ver un listado de números de índice, entre **list all** en el indicador `xtp>`.

Ejemplo:

`list pvc-detailed`

PVC Index Number [1]?1

PVC 1 IN DETAIL

```
-----
Int  PVC      Received      Sent      Dropped
No  State    Pkts  Bytes    Pkts  Bytes    Pkts  Bytes
1   ACTIVE   55    3220    35    2350    15    1870
```

pvcs-all-detailed

Visualiza información detallada para todas las definiciones de PVC.

Ejemplo:

`list pvcs-all-detailed`

LIST OF PVCS

Mandatos de supervisión XTP (Talk 5)

```
-----  
INT Local PVC Received Sent Dropped  
No LCN State Pkts Bytes Pkts Bytes Pkts Bytes  
1 1 ACTIVE 55 3220 35 2350 15 1870
```

svcs Visualiza todas las definiciones de SVC.

Ejemplo:

```
list svcs
```

```
LIST OF SVCS
```

```
-----  
Index Int LOG SVC Local Remote Peer  
No No Chan State DTE Router  
1 1 1 Active 200 401 3.3.3.3  
2 1 1 Active 200 402 3.3.3.3  
3 2 2 Active 200 403 3.3.3.3  
4 2 2 Active 200 404 3.3.3.3
```

svc-detailed

Visualiza información para definiciones de SVC específicos.

Ejemplo:

```
list svc-detailed
```

```
SVC Index Number [1]?1
```

```
SVC 1 IN DETAIL
```

```
-----  
Int LOG SVC Received Sent Dropped  
No Chan State Pkts Bytes Pkts Bytes Pkts Bytes  
1 1 ACTIVE 75 4220 55 3350 20 870
```

svcs-all-detailed

Visualiza información para todas las definiciones de SVC.

Ejemplo:

```
list svcs-all-detailed
```

```
LIST OF SVCS
```

```
-----  
Index Int Log SVC Received Sent Dropped  
No No Chn State Pkts Bytes Pkts Bytes Pkts Bytes  
1 1 1 ACTIVE 4220 55 550 20 870  
2 1 1 ACTIVE 3220 40 2350 15 970  
3 2 2 ACTIVE 4003 50 3892 20 870  
4 2 2 ACTIVE 3967 58 4167 12 800
```

Soporte para la reconfiguración dinámica de la interfaz de red X.25

Esta sección describe la reconfiguración dinámica (DR) en la medida en que afecta a los mandatos Talk 6 y Talk 5.

Delete Interface de CONFIG (Talk 6)

La interfaz de red X.25 no soporta el mandato **delete interface** de CONFIG (Talk 6).

Activate Interface de GWCON (Talk 5)

La interfaz de red X.25 no soporta el mandato **activate interface** de GWCON (Talk5).

Reset Interface de GWCON (Talk 5)

La interfaz de red X.25 no soporta el mandato **reset interface** de GWCON (Talk 5).

Capítulo 41. Utilización de interfaces Frame Relay

Este capítulo describe cómo utilizar la interfaz Frame Relay (FR) e incluye las secciones siguientes:

- “Visión general de Frame Relay”
- “Gestión de la red Frame Relay” en la página 541
- “Velocidades de datos Frame Relay” en la página 543
- “Congestión de circuitos” en la página 546
- “Reserva de ancho de banda en Frame Relay” en la página 551
- “Fragmentación a través de una interfaz Frame Relay” en la página 551
- “Reenvío de voz a través de Frame Relay” en la página 552
- “Visualización del indicador de configuración de Frame Relay” en la página 558
- “Procedimiento de la configuración básica de Frame Relay” en la página 558
- “Habilitación de la gestión de PVC en Frame Relay” en la página 559
- “Habilitación de la gestión de SVC en Frame Relay” en la página 560

Visión general de Frame Relay

El protocolo FR es un método para transmitir paquetes en redes internet combinando la conmutación de paquetes y el compartimiento de puertos X.25 con la alta velocidad y el poco retardo de la conmutación de circuitos de multiplexación de división tiempo (TDM). FR le permite conectar múltiples LAN en un solo enlace WAN de alta velocidad (1,54 Mbps) con múltiples circuitos virtuales (VC) de punto a punto. FR offers the following features:

- *Alta productividad y bajo retardo.* Mediante la utilización de los *aspectos de imagen de memoria* (detección de errores, direccionamiento y sincronización) del protocolo de enlace de datos Link Access Protocol, D-Channel (LAPD), FR elimina todo el proceso de capa de red (Capa 3). Con la sola utilización de los aspectos de imagen de memoria, FR reduce el retardo del proceso de cada trama.
- *Detección de la congestión.* Al recibir una Notificación explícita de congestión hacia atrás (BECN) o una Notificación explícita de congestión hacia adelante (FECN), el direccionador inicia una moderación controlada de la velocidad del tráfico, evitando un cierre completo de la red FR.

El direccionador también puede iniciar una moderación de la velocidad del tráfico cuando recibe un mensaje de congestión de la Gestión de la capa de enlace consolidada (CLLM). CLLM es una parte opcional de los estándares de FR que proporciona información adicional de gestión acerca del funcionamiento de la red frame relay con los DTE conectados.

- *Acceso y control de circuitos.* Como el direccionador reconoce dinámicamente la disponibilidad de circuitos no configurados (circuitos huérfanos), el usuario puede controlar el acceso a estos nuevos circuitos.
- *Opción de gestión de la red.* Cuando la red lo necesite, el protocolo FR puede funcionar con o sin una interfaz de gestión de red local.
- *Multiplexación de protocolos.* Utilizando un VC para pasar múltiples protocolos.
- *La compresión de datos,* que soporta el estándar FRF.9. Consulte la sección “Utilización de compresión de datos” de la publicación *Utilización y configuración de las características* para ver los detalles.
- *El cifrado de datos,* utilizando un esquema de cifrado de propietario. Consulte la sección “Utilización y configuración de encriptación de datos” de la publicación *Utilización y configuración de las características* para ver los detalles.

Utilización de Frame Relay

FR no proporciona la función de corrección de errores o de retransmisión. Para proporcionar una transmisión de datos de extremo a extremo sin errores, FR confía en la inteligencia de los dispositivos del sistema principal.

Red Frame Relay

La red FR consta de la red troncal FR (que consiste en conmutadores FR proporcionados por la portadora FR) que proporciona el servicio FR. El direccionador funciona como el dispositivo de conexión FR. El direccionador encapsula las tramas FR y las direcciona a través de la red basándose en un Identificador de conexión de enlace de datos (DLCI). El DLCI es la dirección de control de acceso al medio (MAC) que identifica el PVC o el SVC entre el direccionador y el dispositivo de destino FR. Por ejemplo, en la Figura 38, el direccionador D recibe paquetes del direccionador B y envía paquetes al mismo mediante el DLCI 16 y el direccionador B recibe paquetes del direccionador D y envía paquetes al mismo mediante el DLCI 19. El proveedor FR es responsable de completar el circuito conectando el DLCI 19, que está conectado al direccionador B, al DLCI 16 conectado al direccionador B. Existe una relación similar entre el direccionador D y el direccionador A utilizando los DLCI 17 y 18, respectivamente.

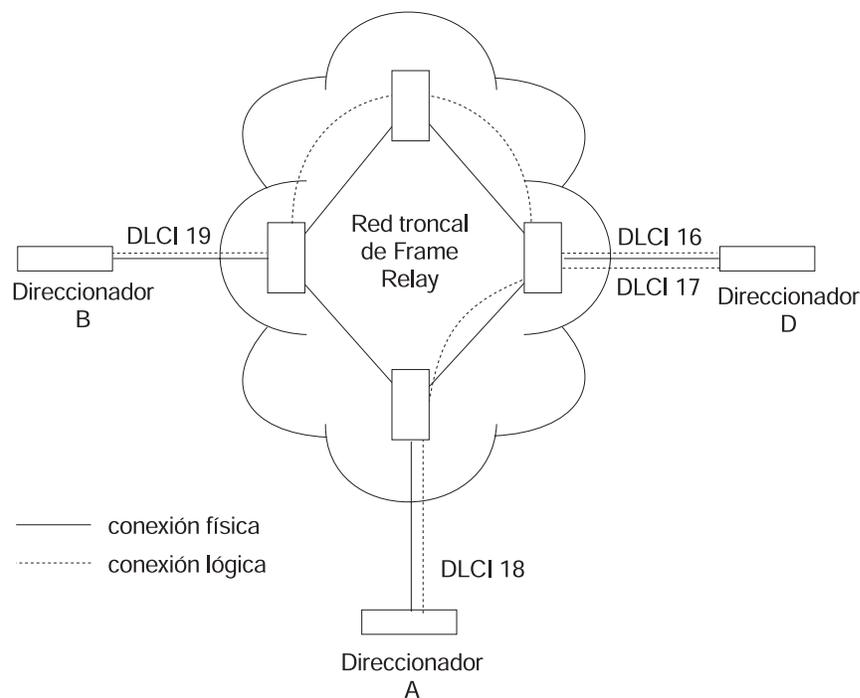


Figura 38. Los DLCI en la red FR

Un DLCI puede tener un significado local o global. Los DLCI locales son significativos en el punto de entrada a la red, pero los DLCI globales son significativos en toda la red. Sin embargo, el DLCI que el direccionador utiliza para direccionar un paquete es el DLCI que el usuario asocia con el destino global o local de la trama. Los DLCI se configuran mediante el proceso de configuración FR o se conocen a través de la gestión FR.

Los PVC FR son conexiones predefinidas utilizadas para direccionar los datos a través de una red FR. El ancho de banda asignado para un PVC de la red es una opción de suscripción y debe estar asignado al PVC, aunque éste no lo utilice.

Una red FR tiene las características siguientes:

- Transporta las tramas transparentemente. La red sólo puede modificar el DLCI, los bits de congestión y la secuencia de comprobación de tramas. Los distintivos del Control de enlace de datos de alto nivel (HDLC) y la inserción del bit cero proporcionan la delimitación, alineación y transparencia de las tramas.
- Detecta la transmisión, el formato y los errores operativos (tramas con un DLCI desconocido).
- Conserva el orden de la transferencia de tramas en VC individuales.
- No reconoce ni retransmite tramas.

Subinterfaces para Frame Relay

Las subinterfaces FR son interfaces lógicas que están asociadas a una interfaz FR. Debe definirse la interfaz FR, conocida como la interfaz base FR, antes de configurar una o varias subinterfaces FR. Se dice que las subinterfaces FR están asociadas a la interfaz base FR.

Después de crear una subinterfaz FR, puede configurar los circuitos a través de ella, tal como lo haría a través de cualquier interfaz FR. Sin embargo, tenga en cuenta que algunas características de las interfaces como, por ejemplo, la compresión y el cifrado, sólo pueden habilitarse en la interfaz base.

La utilización de subinterfaces FR tiene tres ventajas principales:

1. Le permite tener un mayor control de las difusiones a nivel de interfaz (por ejemplo, RIP) y de los filtros a nivel de interfaz.
2. Mejora el uso del redireccionamiento WAN, ya que no es necesario que la interfaz base FR falle antes de hacer una copia de seguridad de un único PVC. Esto se hace definiendo un PVC en una subinterfaz y convirtiendo la subinterfaz en la interfaz primaria para un redireccionamiento WAN alternativo.
3. Le permite añadir dinámicamente los PVC y los SVC una interfaz, sin restablecer la interfaz FR base. Para hacerlo, defina los PVC o los SVC de las subinterfaces en Talk 6 y active las subinterfaces en Talk 5.

El mandato para crear una subinterfaz FR es **add dev fr**.

Ejemplo:

```
Config>add dev fr
Enter the number of Frame Relay Subinterface interfaces [1]?
Adding device as interface 4
Base net for the Frame Relay Subinterface interface(s) [0]? 3
Use "net " command to configure specific Frame Relay Subinterface parameters
```

Circuitos virtuales conmutados Frame Relay

Los Circuitos virtuales conmutados (SVC) proporcionan la posibilidad de implementar el direccionamiento “abreviado” en una red FR, minimizando o eliminando los saltos intermedios del direccionador entre los DTE. La complejidad de la red puede simplificarse y el DTE puede experimentar una mejora en el rendimiento.

Utilización de Frame Relay

Los SVC pueden sustituir a los PVC para conservar el ancho de banda de la red, reduciendo el coste del ancho de banda.

Los estándares de SVC FR son un subconjunto de estándares RDSI y proporcionan muchas de las ventajas de RDSI con menos complejidad.

Se soportan los siguientes protocolos en los SVC FR:

- AppleTalk 2
- ARP
- Bridging
- DECnet IV
- DLSw
- IP/OSPF/RIP/BGP4
- IPX

Los SVC no pueden ser necesarios ni pertenecer a un grupo necesario.

Manejador de tramas Frame Relay

El manejador de tramas FR permite que el 2216 actúe como un conmutador FR. Esta función permite reenviar el tráfico entre los PVC de interfaces FR sin utilizar la función de direccionamiento ni la de puente. Su finalidad principal es permitir reenviar los protocolos de propiedades o de direccionamiento no soportado mediante el dispositivo de red a través de los PVC FR. Puede hacerse esto, por ejemplo, para conectar un dispositivo de red enviando un protocolo de propiedades directamente a un 2216 en lugar de enviarlo a una red FR, para ahorrarse los costes de acceso FR. Después, podría reenviarse el tráfico de propiedades a través de su propio PVC en la red FR al direccionador de destino, que también podría tener un 2216 como componente frontal. El 2216 puede utilizar diferentes PVC a través de la misma interfaz FR para direccionar y puentear el tráfico a través de la red FR a otros destinos. Otro ejemplo de utilización de esta función es como componente frontal de un controlador o un direccionador que no soporta la forma de tráfico FR con un 2216 y permitir que el 2216 realice esta función por él para reducir el número de tramas que la red FR desecha debido a la congestión.

Como parte de la función del manejador de tramas, el 2216 soportará tanto el proceso de congestión explícito (BECN y FECN) como el implícito (eliminaciones de tramas). Si habilita la supervisión de CIR, hace que se controle la CIR de entrada y de salida. Si está habilitada la supervisión de CIR o de la congestión, se impondrá la profundidad de cola de salida configurada para el PVC manejador de tramas. Si se excede el límite de la cola de salida o de la CIR dará como resultado que las tramas tengan el BECN y el FECN establecido en la dirección adecuada y también una condición de eliminación de tramas.

Si la supervisión no está habilitada, no se establecen el BECN ni el FECN y las tramas reenviarán a través de la interfaz siempre que los almacenamientos intermedios de entrada estén disponibles en las interfaces de entrada. Ahora, el 2216 soporta la parte de la red de la interfaz de gestión local (LMI) FR. Esto permite utilizar la LMI en configuraciones de dispositivos de red de atrás a atrás. La LMI de la parte de la red se utiliza con frecuencia en las configuraciones de manejadores de tramas. Sin embargo, no es necesaria. Tenga en cuenta también que puede utilizar la LMI de la parte de la red sin utilizar la función de manejador de tramas en las configuraciones en las que LMI es útil en las configuraciones de direccionador de atrás-atrás.

El reenvío FH y de voz no se pueden utilizar en el mismo circuito.

Utilización de Frame Relay

La Figura 39 muestra una configuración FH típica. En la interfaz 1, los PVC 16 y 18 están definidos como manejadores de tramas junto con el PVC 19 de la interfaz 2 y el PVC 20 de la interfaz 3. Todo el tráfico recibido en estos PVC se direccionará directamente a sus PVC asociados. También aparece la interfaz 1 soportando un PVC DTE. Los datos recibidos a través de este PVC se proporcionarán a la función de direccionamiento adecuada para que se reenvíen a través de cualquier otra interfaz del dispositivo de red.

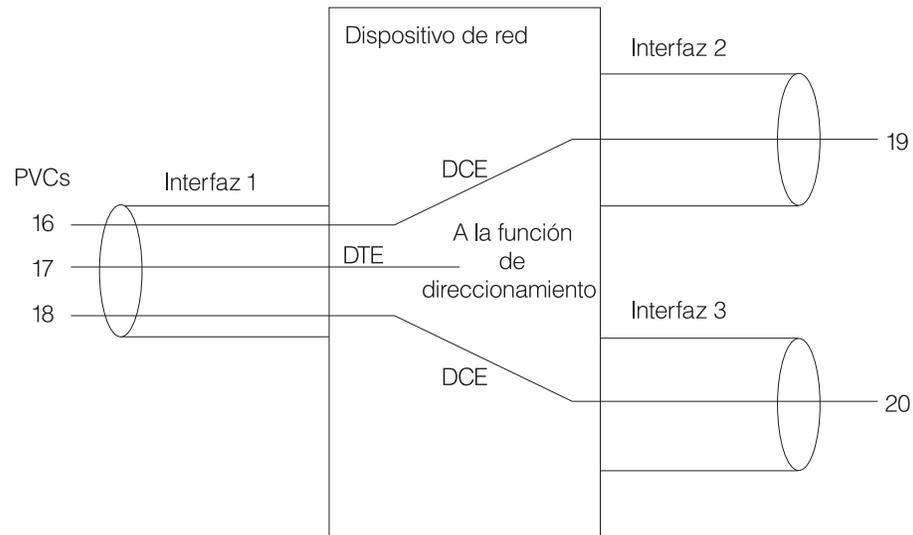


Figura 39. Multiplexación de circuitos DTE y DCE

Inicialización de la interfaz Frame Relay

La Interfaz de gestión local (LMI) se utiliza para determinar el estado de los PVC en una interfaz FR. Si está habilitada una LMI, la interfaz FR se activa cuando se produce un intercambio satisfactorio de tramas LMI entre este direccionador y el nodo FR adyacente; sin embargo, no se pueden recibir datos de otro direccionador ni transmitir datos al mismo hasta que un mensaje de estado LMI indica que el estado del PVC para el DLCI del otro direccionador está activo. También, hay instancias en las que el estado de la interfaz FR se vincula a los estados de PVC y la interfaz no se activa incluso aunque LMI o Q.922 realicen intercambios satisfactorios (para obtener información, consulte la sección “Configuración de los estados de PVC para que afecten al estado de la interfaz Frame Relay” en la página 537).

Si la LMI no está habilitada y los SVC sí, la interfaz FR se activa cuando se produce un intercambio satisfactorio de tramas Q.922 entre el direccionador y el dispositivo adyacente. Todos los PVC se consideran activos en este momento. Sin embargo, los SVC sólo están activos después de un intercambio de activación Q.933 satisfactorio.

El estado de PVC aparece para todos los PVC como activo o inactivo. Un PVC activo ha completado una conexión con un sistema final. Un PVC inactivo no ha completado ninguna conexión con un sistema final porque un sistema final o un conmutador FR está fuera de línea.

Por ejemplo, en la Figura 40 en la página 536, el direccionador B tiene un PVC configurado para el direccionador D. El direccionador B está interactuando satisfactoriamente con la gestión FR a través del conmutador FR B. Puesto que

Utilización de Frame Relay

otro conmutador FR o el sistema final está desactivado, la conexión PVC de extremo a extremo no se ha establecido. El direccionador B recibe un estado inactivo para ese PVC.

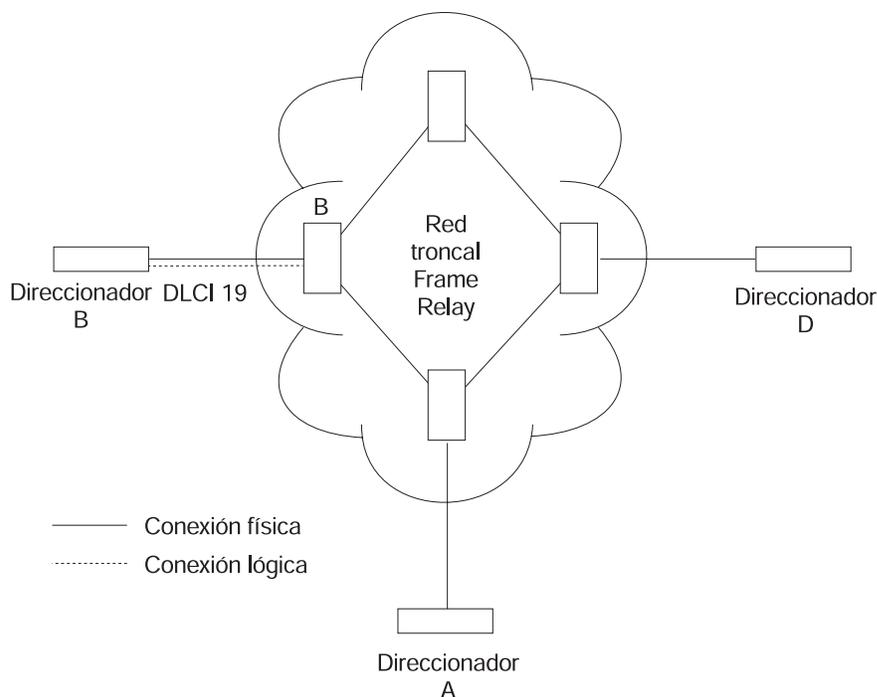


Figura 40. Los DLCI en la red Frame Relay

Las conexiones DSU deben configurarse para que eliminen las señales de Conjunto de datos preparado (DSR), Preparado para transmitir (CTS) o Detección de portadora de datos (DCD) si se pierde la conexión de red.

Circuitos huérfanos

Un circuito virtual permanente huérfano es cualquier PVC que no está configurado para el direccionador, pero que se reconoce indirectamente a través de la conexión de la interfaz de gestión local (LMI) con el proveedor de Frame Relay. Por ejemplo, la Figura 41 en la página 537 supone que el direccionador B tiene un PVC configurado para el direccionador D y ninguno para el direccionador A. Se puede conseguir un circuito entre los direccionadores A y B sin configurar Circuitos virtuales permanentes (PVC) en el direccionador. El proveedor de FR configura un circuito utilizando los Identificadores de conexión de enlace de datos (DLCI) entre los puertos a los que están conectados el direccionador A y el direccionador B. Los direccionadores A y B, cuando se comunican a través de la LMI, piden el estado y obtienen como respuesta un mensaje que indica la presencia de Identificadores de conexión de enlace de datos (DLCI). Los PVC reconocidos de esta forma se llaman *circuitos huérfanos*. El direccionador B reconocería el PVC para el direccionador A a partir de los mensajes de LMI y lo clasificaría como huérfano.

Los PVC huérfanos se tratan igual que los circuitos configurados excepto en que el usuario puede habilitar o inhabilitar su uso con los mandatos **enable orphan-circuit** y **disable orphan-circuit**.

Nota: Todos los PVC huérfanos se utilizarán como circuitos DTE, no como FH. Los PVC huérfanos no se pueden utilizar para el reenvío de voz ni para APPN®.

Mediante la inhabilitación de circuitos huérfanos, se añade una medida de seguridad a la red impidiendo cualquier entrada no autorizada en la red desde un circuito no configurado. Mediante la habilitación de circuitos huérfanos, se permite que el direccionador reenvíe paquetes a través de circuitos que el usuario no ha configurado. Los paquetes que normalmente se eliminarían, ahora se reenvían.

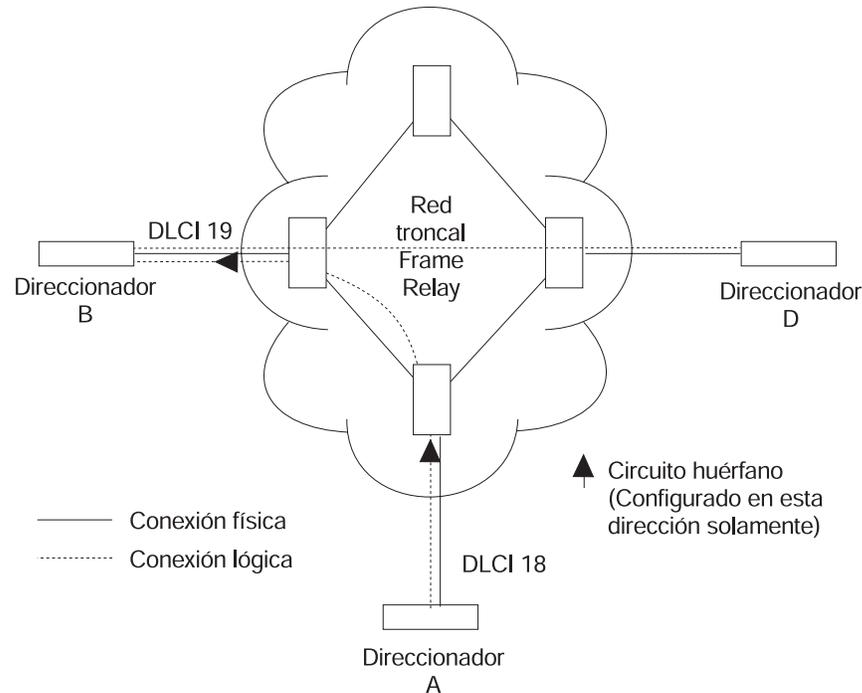


Figura 41. Circuito huérfano

Un circuito virtual conmutado huérfano es un SVC que no está configurado para el direccionador pero que se crea cuando se recibe una llamada de entrada para el mismo. Esto es similar a la Figura 41. Sin embargo, se utilizan los mensajes Q.933 en lugar de la LMI para generar el circuito y asociar los parámetros adecuados al mismo. Los SVC huérfanos se tratan igual que los SVC configurados excepto en que el usuario puede habilitar o inhabilitar su utilización con la opción de llamada de entrada del mandato **enable switched-virtual-circuit**.

Configuración de los estados de PVC para que afecten al estado de la interfaz Frame Relay

Puede controlar el funcionamiento de la interfaz FR realizando una de las acciones siguientes:

- Habilitando la característica *Sin PVC*
- Configurando los *PVC necesarios*
- Configurando los *grupos de PVC necesarios*

Mediante la habilitación de la característica *Sin PVC*, la interfaz FR pasa a estar inactiva cuando no hay ningún PVC activo en la interfaz. Si hay un PVC activo como mínimo, la interfaz FR se activa al producirse un intercambio LMI satisfactorio entre el direccionador y el conmutador FR.

Utilización de Frame Relay

Puede configurar un PVC como un *PVC necesario*. Si un PVC es necesario pero no está en un grupo, la interfaz FR pasa a estar inactiva cuando se inactiva el PVC. Cuando se activa un PVC, la interfaz también se activa después de un intercambio satisfactorio de tramas LMI entre el direccionador y el conmutador FR.

Si varios PVC son necesarios y no están en un grupo de PVC, la interfaz no se activa hasta que todos los PVC necesarios están activos.

Si un PVC necesario pertenece a un grupo PVC, la interfaz FR pasa a estar inactiva cuando todos los PVC del grupo de PVC están inactivos. Si como mínimo un PC del grupo está activo, la interfaz también se activa después de un intercambio satisfactorio de tramas LMI entre el direccionador y el conmutador FR. Si hay varios grupos de PVC, la interfaz no se activa hasta que al menos un PVC de cada grupo se activa.

Un *grupo de PVC necesario* es un grupo de circuitos asociados por el nombre, donde el *nombre* es el nombre del grupo de PVC necesario.

Estas características pueden utilizarse con el Redireccionamiento de WAN para que pueda activarse un enlace alternativo si todos los PVC, los PVC necesarios o un grupo de PVC, se inactivan en el enlace FR primario.

Opción de interfaz de punto a punto

Se puede habilitar el punto a punto para las interfaces FR y para las subinterfaces FR. Esta opción indica si la interfaz es de punto a punto desde el punto de vista de IP. Si configura una interfaz FR como de punto a punto, puede ejecutarse un IP sin numerar en la interfaz.

Trama Frame Relay

Una trama FR consta de un campo de dirección de tamaño fijo con datos de usuario encapsulados de tamaño variable. La Figura 42 ilustra un formato de trama FR.

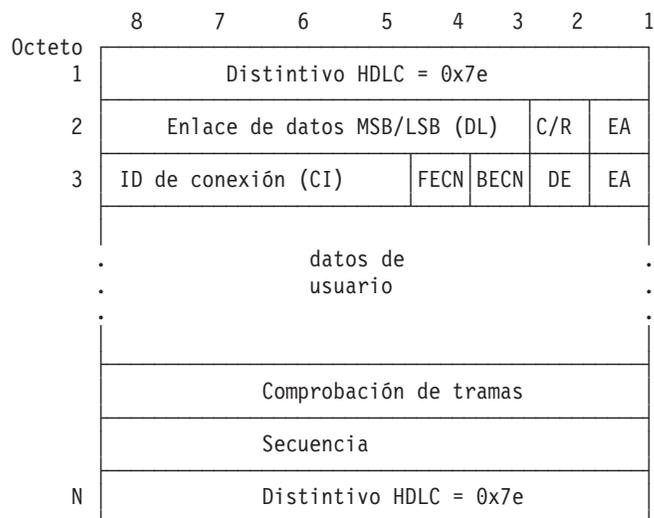


Figura 42. Formato de trama Frame-Relay

Distintivos HDLC

Ubicados en el primer y en el último octeto, estos distintivos indican el principio y el final de la trama.

Identificador de conexión de enlace de datos (DLCI)

Este ID de direccionamiento de 10 bits reside en los bits 3 a 8 del octeto 2 y en los bits 5 a 8 del octeto 3. El DLCI es la dirección MAC del circuito. El DLCI permite al usuario y a la gestión de la red identificar que la trama es de un PVC en particular. El DLCI permite la multiplexación de varios PVC en un enlace físico.

Mandato/Respuesta (C/R)

La utilización de este campo no está definida en los estándares FR y el campo se pasa transparentemente a través de la red.

Dirección extendida

Esta versión de FR no soporta el direccionamiento extendido.

Notificación explícita de congestión hacia adelante (FECN)

La red troncal FR establece este bit en 1 para notificar al usuario que recibe la trama que se está produciendo congestión para el PVC en la dirección en que se envía la trama. Puede configurar el dispositivo para moderar la velocidad de la transmisión de datos en la dirección en la que recibe una FECN utilizando el mandato **enable throttle-transmit-on-fecn**. También puede establecer el bit BECN en las tramas de datos enviadas al originador de la FECN utilizando el mandato **enable notify-fecn-source**.

El Direccionamiento de alto rendimiento (HPR) APPN utiliza la detección del establecimiento de este bit para permitir que el algoritmo de control de la congestión y el flujo basado en la velocidad adaptada de Rapid Transport Protocol ajuste la velocidad del envío de datos. Este algoritmo impide las ráfagas y la congestión del tráfico, manteniendo un alto nivel de productividad.

Notificación explícita de congestión hacia atrás (BECN)

La red troncal FR establece este bit en 1 para notificar al usuario que las tramas enviadas por este direccionador para este PVC han encontrado una congestión. El direccionador inicia una *moderación de la velocidad* hasta que sea igual o inferior a la CIR definida por el usuario cuando está habilitada la supervisión de CIR o de la congestión. La CIR para un PVC la suministra el proveedor de servicio FR y se configura utilizando el mandato **add permanent-virtual-circuit**.

Elegibilidad para eliminar (DE)

La red FR puede eliminar los datos transmitidos que exceden la CIR de un PVC. El direccionador puede establecer el bit DE para indicar que parte del tráfico debe considerarse elegible para su eliminación. Si procede, la red FR eliminará las tramas marcadas como elegibles para eliminar, lo que puede permitir que las tramas que no estén marcadas como elegibles para eliminar pasen a través de la red. Para identificar el tráfico elegible para eliminar:

1. Configure BRS en la interfaz FR y cualquier circuito FR que tenga tráfico que defina como elegible para eliminar.
2. Asigne un protocolo o filtro a la clase de tráfico BRS utilizando el mandato **assign**. Se especifica si debe establecerse el bit DE para el tráfico de este protocolo o filtro.

Datos de usuario

Este campo contiene el paquete de protocolos que se está transmitiendo. Este campo puede contener un máximo de 8188 octetos; sin embargo, la secuencia de comprobación de tramas (FCS) sólo puede detectar con eficacia los errores en un

Utilización de Frame Relay

máximo de 4096 octetos de datos. Los datos de protocolo van precedidos por la cabecera de encapsulación de FR, tal como se define en RFC 1490 y RFC 2427.

Secuencia de comprobación de tramas

Este campo es la comprobación de redundancia cíclica (CRC) estándar de 16 bits que utilizan las tramas HDLC y LAPD. Este campo detecta los errores de bits que se producen en los bits de la trama entre el distintivo de apertura y FCS.

Nota: Nota: Con el adaptador HSSI hay una Secuencia de comprobación de tramas (FCS) de 32 bits opcional.

Nota: Puede configurar la utilización de un CRC de 32 bits para la interfaz FR en un adaptador HSSI.

Reenvío de tramas a través de la red Frame Relay

Cuando el protocolo FR recibe un paquete para encapsulación, compara la dirección de red del paquete con las entradas de la antememoria de Address Resolution Protocol (ARP). Si la antememoria ARP contiene el número de DLCI que coincide con la dirección de red, el protocolo FR encapsula el paquete en una trama y la transmite al DLCI local especificado. Si la antememoria ARP no contiene una coincidencia, el protocolo FR envía una petición ARP a todos los PVC configurados en la interfaz. Cuando el punto final adecuado responde con una respuesta ARP, el protocolo FR añade su DLCI local que ha recibido la respuesta ARP a la antememoria ARP. Entonces se encapsulan los paquetes de datos subsiguientes direccionados a la misma dirección de red en una trama y se envía a su DLCI local.

Direcciones de protocolo

Las direcciones de protocolo pueden correlacionarse estáticamente con las direcciones de PVC de la red FR o SVC utilizando los nombres configurados localmente o pueden descubrirse dinámicamente mediante Inverse ARP o ARP. (Para obtener más información sobre ARP e Inverse ARP, consulte la publicación *Consulta de configuración y supervisión de protocolos*.) Cualquier método es dependiente de protocolo, tal como se ilustra en la Tabla 68.

Nota: También se hace referencia a las direcciones de protocolo estáticas como entradas ARP estáticas. Una entrada ARP estática se añade a la configuración con el mandato **add protocol-address**.

Tabla 68. Correlación de direcciones de protocolo

Tipo de protocolo	Utilización de ARP e		VC configurado en la configuración del protocolo
	Inverse ARP	Correlación estática	
AP2	Sí	Sí	No
IP	Sí	Sí	No
IPX	Sí	Sí	No
Banyan VINES**	No	No	No
DNA IV	Sí	Sí	No
OSI*, **	No	No	Sí

* Debe configurar OSI a nivel de protocolo para correlacionar la dirección de protocolo con el PVC FR.
** No está soportado cuando se utilizan los SVC.

Emulación de multidifusión y difusión de protocolo

La emulación de multidifusión es una característica opcional que permite que los protocolos que necesitan la multidifusión como, por ejemplo, ARP funcionen correctamente a través de la interfaz FR. Con la emulación de multidifusión, se transmite una trama de multidifusión en cada PVC activo. Mediante la utilización de los mandatos **enable** y **disable multicast**, puede activar o desactivar esta característica. Los protocolos que utilizan la multidifusión son AP2, ARP, Banyan VINES, DNA4, IP e IPX.

La difusión de protocolo es otra característica opcional que permite que el protocolo IP RIP funcione correctamente a través de la interfaz FR. Mediante la utilización de los mandatos **enable protocol-broadcast** y **disable protocol-broadcast**, puede activar o desactivar esta característica.

Para los protocolos que soportan ARP/InARP a través de FR, FR sólo realizará una multidifusión de los paquetes de protocolos en un circuito si se ha reconocido o configurado una dirección de protocolo para ese circuito.

La multidifusión también se puede habilitar o inhabilitar para un SVC individual. Utilice la opción de multidifusión de **add switched-virtual-circuit**.

Gestión de la red Frame Relay

El proveedor de la red troncal FR proporciona la gestión de red FR. Es responsabilidad de la gestión proporcionar a las estaciones finales FR (direccionadores) la información de estado y configuración relativa a los PVC disponibles en la interfaz.

Para los PVC, el protocolo FR soporta las entidades de gestión ANSI T1.617 Anexo D, ITU-T Q.933 Anexo A (también llamada CCITT Q.933 Anexo A) e Interim Local Management Interface (LMI). Puede activar y desactivar estas entidades utilizando los mandatos de configuración LMI **enable** y **disable**. Una vez haya habilitado la LMI, utilice el mandato **set** para seleccionar el estándar de LMI que se ha de utilizar y el tipo de red LMI. El estándar de LMI, ANSI, CCITT o REV1, debe ser compatible con el nodo FR adyacente. El tipo de red LMI determina si FR sólo pide el estado del nodo adyacente, sólo proporciona el estado al nodo adyacente o realiza las dos acciones simultáneamente. El tipo de red LMI también debe ser compatible con el nodo FR adyacente. Específicamente, la LMI FR proporciona la información siguiente:

- Notificación de los PVC adicionales (huérfanos) y si están activos o inactivos o la notificación de cualquier supresión de PVC.
- Notificación de la disponibilidad de un PVC configurado. La disponibilidad de un PVC está relacionada indirectamente con la participación satisfactoria del punto final del PVC en el proceso *sondeo de señal de actividad*, que se detalla en la sección "Informe de verificación de la integridad del enlace" en la página 542.
- Verificación de la integridad del enlace físico entre la estación final y la red utilizando un intercambio de número de secuencia de *mantener activo*.

Aunque la interfaz FR soporte la gestión de red PVC, no es necesario ejecutar la gestión en la red troncal FR para que la interfaz funcione a través de la red troncal FR. Por ejemplo, puede inhabilitar la gestión para las configuraciones de atrás a atrás; sin embargo, no siempre es necesario ya que FR proporciona la parte del usuario y la parte de la red del protocolo de gestión LMI.

Utilización de Frame Relay

Para los SVC, el protocolo FR soporta FRF 4 (Frame Relay Forum Implementation Agreement 4). Esto incluye una implementación de ANSI Q.922 y un subconjunto de ANSI Q.933. Q.922 proporciona la verificación de la integridad del enlace físico entre el direccionador y la red. Q.933 proporciona un medio para establecer y desconectar los SVC en la red. Q.922 y Q.933 están siempre habilitados cuando se utilizan los SVC.

Informe del estado de la gestión

Cuando se solicita, LMI FR proporciona dos tipos de informes de estado, un informe de estado completo y un informe de verificación de la integridad del enlace. El informe de estado completo proporciona información acerca de todos los PVC que la interfaz conoce. Un informe de verificación de la integridad del enlace verifica la conexión entre una estación final específica y un conmutador de la red. Todas las consultas y respuestas de estados se envían al DLCI 0 para ANSI T1.617 Anexo D e ITU-T Q.933 Anexo A o al DLCI 1023 para la gestión LMI interina.

Informe de estado completo

Cuando la interfaz FR necesita un informe de estado completo, el protocolo FR del direccionador envía un mensaje de consulta de estado a la red troncal FR pidiendo un informe de estado completo. Un mensaje de consulta de estado es una petición del estado de todos los PVC de la interfaz. Cuando se recibe esta petición, la gestión FR debe responder con un informe de estado completo que consiste en el elemento de verificación de la integridad del enlace y un elemento de información del estado del PVC para cada PVC (consulte “Informe de verificación de la integridad del enlace”).

El elemento de información de estado del PVC contiene la información siguiente: el número de DLCI local para el PVC en particular, el estado del PVC (activo o inactivo) y si el PVC es nuevo o un PVC existente que la gestión ya conoce.

Nota: El número de PVC suministrados en la interfaz FR se limita al tamaño de trama de red y la cantidad de elementos de información de PVC individual que pueden caber en un informe de estado completo. Por ejemplo, 202 es el número máximo de PVC para una red con un tamaño de trama de 1 K.

Informe de verificación de la integridad del enlace

El informe de verificación de la integridad del enlace, al que a veces se llama *sondeo de señal de actividad*, contiene el elemento de verificación de la integridad del enlace. En este elemento es donde tiene lugar el intercambio de números de secuencia de envío y recepción. Mediante el intercambio de los números de secuencia, la gestión y la estación final pueden evaluar la integridad del enlace síncrono. El número de secuencia de envío es el número de secuencia de envío actual del originador del mensaje. El receptor consulta este número y lo compara con el último número de secuencia de envío para verificar que se haya incrementado correctamente. El número de secuencia de recepción es el último número de secuencia de envío que el originador ha enviado a través de la interfaz. Es responsabilidad del receptor colocar una copia del número de secuencia de envío en el campo del número de secuencia de recepción. De esta manera el originador puede asegurarse de que el receptor recibe e interpreta las tramas correctamente.

Cuando una estación final no puede participar en este proceso de sondeo, se notifica a todas las estaciones finales remotas con PVC conectados lógicamente, mediante el mecanismo de informe de estado completo de la gestión, de que el PVC está inactivo.

Gestión de capa de enlace consolidada (CLLM)

CLLM es una función de gestión FR opcional que no está ampliamente soportada en la industria pero que han adoptado algunos fabricantes de conmutadores FR. CLLM proporciona parte de la misma información de gestión proporcionada por LMI, en particular, la notificación de las insuficiencias. CLLM se utiliza principalmente para proporcionar la notificación de congestión asincrónica de los PVC a los dispositivos de conexión. Un solo mensaje CLLM puede indicar la falta o la congestión de múltiples PVC. El protocolo FR soporta los estándares siguientes para CLLM: ANSI T1.618, ITU-T (CCITT) Q.922 Anexo A e ITU-T (CCITT) X.36 Anexo C.

Velocidades de datos Frame Relay

Esta sección presenta las velocidades de datos para los circuitos virtuales permanentes (PVC) y los circuitos de virtuales conmutados (SVC).

Velocidad de información confirmada (CIR)

La CIR es la velocidad de los datos que la red confirma para dar soporte al VC bajo condiciones normales, sin congestión. Se proporciona una CIR (por el proveedor de red troncal FR) a cualquier VC que esté configurado o que se reconozca. La CIR es una parte del ancho de banda total del enlace físico de 0 o entre 300 bps y 2 Mbps* reservada para el VC. El valor de 64 kbps para un solo canal DS0 es lo más común.

***Nota:** El valor máximo de CIR para una interfaz FR de un adaptador HSSI es 52 Mbps.

La CIR se define con los mandatos de configuración **add permanent-virtual-circuit**, **change permanent-virtual-circuit**, **add frame-handler**, **change frame-handler**, **add switched-virtual-circuit** o **change switched-virtual-circuit**. También puede cambiar dinámicamente la CIR con el mandato de consola **set circuit**. También puede establecer la CIR por omisión para todos los circuitos Frame Relay en esta interfaz utilizando el mandato **set CIR-defaults**.

Algunos conmutadores FR permiten configurar un valor 0 para la CIR. Cuando la CIR es igual a 0, se reserva poco o ningún ancho de banda en la red troncal FR para el VC y el tráfico del VC utiliza un ancho de banda no reservado.

CIR de circuito virtual permanente huérfano

El direccionador asigna una CIR a circuitos huérfanos basándose en los valores por omisión de CIR configurados a nivel de interfaz. Si se basa en que el circuito huérfano direcciona datos importantes, y los valores de CIR, Bc y Be del proveedor de la red son diferentes de los valores configurados a nivel de interfaz, se recomienda definir un PVC en lugar de un circuito huérfano. Haciendo esto, puede asignar una CIR que la red confirme su soporte.

Utilización de Frame Relay

Tamaño de ráfaga confirmado (Bc)

El *tamaño de ráfaga confirmado (Bc)* es la cantidad máxima de datos (en bits) que la red confirma entregar durante un *intervalo de tiempo calculado (Tc)*. El Tc es igual a la Bc dividido por la CIR ($Tc = Bc / CIR$). Si configura 0 para la CIR, FR utiliza el valor de 1 segundo para el Tc.

Por ejemplo, si establece la CIR de un VC en 9600 bps y el tamaño de ráfaga confirmado en 14 400 bits, el período de tiempo es de 1,5 segundos (14 400 bits / 9600 bps = 1,5 segundos). Esto significa que el VC tiene permitido transmitir un máximo de 14 400 bits en 1,5 segundos.

Nota: El Tc mínimo soportado por FR es 0,03 de segundo.

Este parámetro es importante debido a la relación existente entre el tamaño de ráfaga confirmado y el tamaño máximo de trama. Si el tamaño máximo de trama en bits es superior al tamaño de ráfaga confirmado, la red puede eliminar las tramas cuyo tamaño exceda del tamaño de ráfaga confirmado. Por lo tanto, el tamaño de ráfaga confirmado debe ser mayor o igual al tamaño máximo de trama. También debe ser igual al tamaño de ráfaga configurado con el proveedor de la red.

Utilice los mandatos de configuración **add permanent-virtual-circuit**, **change permanent-virtual-circuit**, **add frame-handler**, **change frame-handler**, **add switched-virtual-circuit** o **change switched-virtual-circuit** para establecer el tamaño de ráfaga confirmado. Puede utilizarse el mandato de consola **set circuit** para cambiar dinámicamente el tamaño de ráfaga confirmado. También puede establecer el tamaño de ráfaga confirmado por omisión para todos los circuitos FR de esta interfaz utilizando el mandato **set CIR-defaults**.

El dispositivo asigna a los circuitos huérfanos un tamaño de ráfaga confirmado basándose en el valor por omisión que establezca con el mandato **set CIR-defaults**. Si configura 0 para CIR, el tamaño de ráfaga confirmado (Bc) también es igual a 0.

Tamaño de exceso de ráfaga (Be)

El *tamaño de exceso de ráfaga (Be)* es la cantidad máxima de datos no confirmados que el direccionador puede transmitir en un PVC que exceden el Bc durante el Tc ($Tc = Bc / CIR$) cuando CIR y Bc no son cero. Cuando la CIR = 0, FR utiliza el valor de 1 segundo para Tc.

La red entrega este exceso de datos con una probabilidad de éxito inferior a los datos de tamaño de ráfaga confirmado. Sólo establezca un valor superior a cero de Be si desea arriesgarse a que se eliminen datos y aceptar su efecto en el rendimiento del protocolo de capa superior. El Be debe ser igual al valor configurado con el proveedor de la red.

Utilice los mandatos **add permanent-virtual-circuit**, **change permanent-virtual-circuit**, **add frame-handler**, **change frame-handler**, **add switched-virtual-circuit** o **change switched-virtual-circuit** durante la configuración de frame relay para establecer el tamaño de exceso de ráfaga. También puede utilizar el mandato de consola **set circuit** para cambiar dinámicamente el tamaño del exceso de ráfaga. Los circuitos huérfanos recibirán un tamaño de exceso de ráfaga por omisión igual al valor establecido en el mandato **set CIR-defaults**. Si configura 0 para CIR, debe configurar un valor distinto de cero para el tamaño de exceso de ráfaga (Be). También puede establecer el tamaño de exceso de ráfaga por omisión para todos los circuitos FR de esta interfaz utilizando el mandato **set CIR-defaults**.

Velocidad de línea

La *velocidad de línea* es la velocidad de línea de la interfaz.

La velocidad de línea de la interfaz FR se configura utilizando el mandato de configuración **set line-speed**. La velocidad de línea debe configurarse cuando se utiliza el cronometraje interno. Sin embargo, se recomienda configurar una velocidad de línea para el cronometraje externo ya que el direccionador utiliza la velocidad de línea como la velocidad máxima de información cuando se habilita la supervisión de la congestión. También, algunos protocolos utilizan la velocidad de línea configurada de una interfaz al calcular el coste de una ruta.

La velocidad de línea no se puede configurar en una interfaz de circuito de marcación FR. Si el circuito de marcación está correlacionado con una interfaz base RDSI, se utilizan 64 kbps como velocidad de línea.

Para circuitos de marcación que utilizan T1/E1 canalizados como red base, la velocidad de línea es 64 kbps multiplicado por el número de períodos de tiempo asignados o 56 kbps si ha establecido el ancho de banda del circuito canalizado en 56 kbps. Por ejemplo, si establece el número de períodos de tiempo para un circuito canalizado en 3, la velocidad de línea es 192 kbps (3 * 64 kbps).

Si el circuito de marcación se correlaciona con una interfaz base V.25bis, se utiliza la velocidad de línea de la interfaz V.25bis para el circuito de marcación FR.

Velocidad mínima de información

La *velocidad mínima de información (IR)* es la velocidad mínima de datos para un VC a la que el direccionador baja cuando se le notifica la congestión. La IR mínima se establece como un porcentaje de la CIR utilizando el mandato de configuración **set ir-adjustment**. Puede cambiarse dinámicamente utilizando el mandato de consola **set ir-adjustment**. Si configura CIR igual a 0, la IR mínima es 1500 bps.

Velocidad máxima de información

La *velocidad máxima de información* es la velocidad máxima de los datos a la cual el direccionador transmite para un VC. Si la característica de supervisión de CIR está habilitada y la CIR y Bc no son cero, la velocidad máxima de información se calcula utilizando CIR, Bc y Be de la manera siguiente:

$$(Bc + Be) \text{ por intervalo } Tc$$

Si la característica de supervisión de CIR está habilitada y la CIR y Bc están configurados igual a 0, la velocidad máxima de información es igual al tamaño de exceso de ráfaga (Be) por segundo.

Si la característica de supervisión de CIR no está habilitada, la velocidad máxima de información es igual a la velocidad de línea.

Velocidad variable de información

La *velocidad variable de información (VIR)* va desde la IR mínima configurada hasta la IR máxima calculada cuando se habilitan las características de supervisión de CIR y supervisión de la congestión. La VIR se reduce gradualmente hasta la velocidad mínima de información cuando se notifica al direccionador una congestión en un circuito y se aumenta gradualmente hasta la velocidad máxima de información cuando el direccionador deja de recibir notificaciones de congestión. Mediante la utilización del mandato de configuración **set ir-adjustment** se

Utilización de Frame Relay

configura el porcentaje de la velocidad de información por el que debe reducirse la VIR cuando se notifica una congestión al direccionador. También puede utilizar este mandato para configurar el porcentaje de velocidad de información por el que debe aumentarse gradualmente la VIR cuando finaliza la congestión.

Para evitar la carga por impulsos en la red, el direccionador establece inicialmente la VIR en la CIR cuando se activa el VC. Si configura 0 para CIR, la VIR se establece inicialmente en el exceso de ráfaga (Be) multiplicado por el porcentaje de ajuste MIR. Por ejemplo, si Be se establece en 64 000 y el porcentaje de ajuste MIR se establece en 25%, la VIR inicial sería igual a 16 000 bps.

Realmente, la VIR puede exceder el valor máximo en un caso. Si la longitud de una trama en bits es superior a la IR máxima, FR transmite la trama de todas formas.

Nota: Los circuitos Frame Handler (FH) no utilizan ninguna VIR. La velocidad de envío para un circuito FH permanece en la velocidad máxima confirmada de envío para el circuito.

Congestión de circuitos

Nota: Los circuitos FH, como otros circuitos, utilizan las tramas FR para determinar cuándo se produce congestión y para notificarla a los direccionadores. Sin embargo, tienen sus propios métodos para supervisar y manejar la congestión del circuito. Consulte la sección “Congestión del circuito Frame Handler” en la página 549 para obtener más información.

La congestión de circuitos se produce por una de las razones siguientes:

- El remitente transmite más rápido que la productividad permitida
- El receptor va demasiado lento al procesar las tramas
- Se congestiona un enlace de red troncal intermedio, provocando que el remitente transmita más rápido que lo que permite la productividad disponible.

Si se produce congestión en el circuito, la red debe eliminar paquetes o cerrarse o ambos.

En respuesta a la congestión de circuitos, el direccionador implementa una *moderación de la velocidad*, que aminora por fases la transmisión de paquetes hasta la IR mínima configurada. La moderación de la velocidad se produce durante las condiciones siguientes:

- Se produce una congestión de circuito.
- El direccionador es el remitente de las tramas.
- Está habilitada la supervisión de CIR o de la congestión.

Los temas siguientes explican la supervisión de las velocidades de datos FR y la congestión del circuito.

Supervisión de CIR

La supervisión de CIR es una característica FR opcional que puede establecer para cada interfaz, para impedir que el direccionador cree condiciones de congestión en la red FR. La supervisión de CIR permite que la VIR para un VC esté entre las IR mínima y máxima configuradas.

La supervisión de CIR se configura con el mandato de configuración **enable cir-monitor** y está inhabilitada por omisión. La supervisión de CIR, cuando está

habilitada, prevalece sobre la supervisión de la congestión. También se puede habilitar o inhabilitar dinámicamente la supervisión de CIR utilizando los mandatos de consola **enable cir-monitor** y **disable cir-monitor**.

Supervisión de la congestión

La supervisión de la congestión es una característica opcional, establecida por interfaz, que permite que la VIR de los VC varíe en respuesta a la congestión de la red. La VIR asume los valores entre la IR mínima y la IR máxima de la velocidad de línea. La supervisión de la congestión está habilitada por omisión. Puede inhabilitarse con el mandato de configuración **disable congestion-monitor** y volverse a habilitar con el mandato **enable congestion-monitor**. También se puede habilitar o inhabilitar dinámicamente la supervisión de la congestión utilizando los mandatos de consola **enable congestion-monitor** y **disable congestion-monitor**.

La supervisión de CIR, si está habilitada, prevalece sobre la supervisión de la congestión. Si están inhabilitadas la supervisión de CIR y la supervisión de la congestión, la VIR para cada VC de la interfaz se establece en la velocidad de línea y no se reduce en respuesta a una congestión de la red.

Nota: Incluso con la compresión habilitada, el dispositivo utiliza el tamaño de tramas no comprimido para determinar si se está excediendo la VIR.

Notificación y evitación de la congestión

Si se produce una congestión, la red troncal FR es responsable de la notificación al remitente y al receptor mediante el envío de una señal FECN o BECN. FECN y BECN son bits que se establecen en una trama para notificar a los DTE de cada extremo de un VC que se está produciendo la congestión. FECN indica que la congestión se está produciendo en la misma dirección de la que se ha recibido la trama; el remitente está provocando la congestión. BECN indica que las tramas que envía este DTE están provocando la congestión de la red.

Opcionalmente, la red puede utilizar mensajes CLLM para transportar información de congestión para los PVC. Los mensajes CLLM sólo se envían al origen de la congestión y el DTE debe tratarlos de manera similar que los mensajes BECN.

El ejemplo de la Figura 43 en la página 548 muestra una condición de congestión en el conmutador B cuando se envían las tramas del direccionador X al direccionador Y. La red troncal FR notifica al direccionador X que las tramas que envía encuentran una congestión estableciendo el bit BECN en las tramas enviadas al direccionador X. La red troncal FR también notifica al direccionador Y que las tramas que recibe han encontrado una congestión estableciendo el bit FECN.

Si el direccionador recibe una trama que contiene una BECN, es responsabilidad del mismo moderar la velocidad variable de información (VIR) del VC si está habilitada la supervisión de CIR o la supervisión de la congestión. El direccionador hace esto gradualmente a medida que recibe tramas consecutivas con una BECN hasta que se alcanza la IR mínima o llega una trama sin una BECN. Los conmutadores FR establecen con frecuencia una BECN en múltiples tramas después de alcanzar el umbral de congestión. Para que FR evite una sobrerreacción a la congestión de la red cuando la red establece múltiples tramas con una BECN, FR reducirá la VIR de un VC una vez cada segundo como máximo. Esto permite reducir la VIR gradualmente. Cuando el direccionador recibe tramas consecutivas sin ninguna BECN, la VIR aumenta gradualmente hasta la IR máxima.

Utilización de Frame Relay

Dependiendo del funcionamiento de la red FR, puede que sea necesario que el dispositivo reduzca la VIR del VC cuando el dispositivo reciba una FECN para minimizar la cantidad global de tráfico que se ofrece a la red lo más rápidamente posible. Reduciendo la carga global de la red se reduce el número de paquetes eliminados de todos los VC para aligerar la congestión. La habilitación del parámetro **throttle-transmit-on-fecn**, junto con las opciones de supervisión de CIR o de la congestión, hace que el dispositivo trate una FECN como una BECN y reduzca la congestión global de la red FR cuando se reciba cualquier notificación de congestión. Sólo utilice el parámetro **throttle-transmit-on-fecn** en redes FR cuyos métodos de puesta en cola no proporcionen almacenamientos intermedios dedicados para la entrada y la salida. Si se habilita **throttle-transmit-on-fecn**, FR reducirá la VIR de un VC como mucho una vez cada segundo por cada BECN o FECN recibida.

Algunos conmutadores de red FR establecen una FECN para indicar una congestión pero no establecen la BECN. Para proporcionar la notificación de la congestión al origen de la misma, habilite el parámetro **notify-fecn-source** que permite que el dispositivo establezca la BECN en las tramas que transmite a través de un VC en el que ha recibido una FECN. Esta acción proporciona una señal al dispositivo que está provocando la congestión de la red para que modere la VIR del VC.

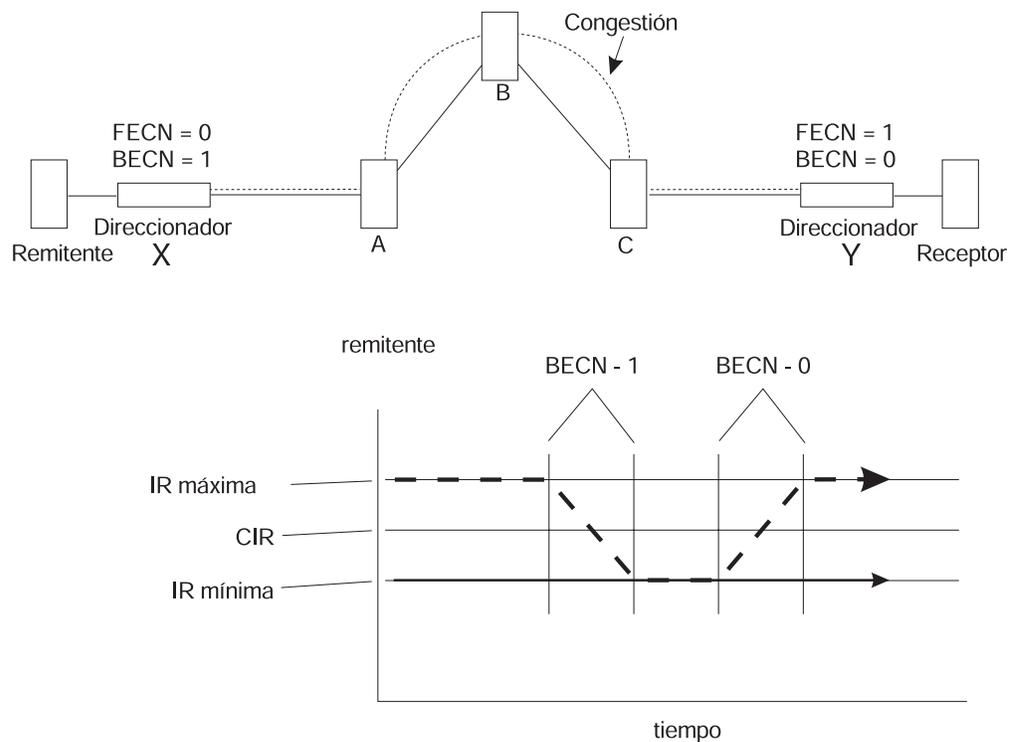


Figura 43. Notificación de congestión y moderación de la velocidad

Nota: Si se configuran múltiples DLCI entre dos estaciones finales cuando se produce la congestión, es posible que se utilice un segundo DLCI para transmitir datos a una productividad superior hasta que se corrija la condición de congestión del primer DLCI.

De manera similar, si el proveedor de la red soporta CLLM, puede configurar FR para que *modere su velocidad* de transmisión para los PVC contenidos en un

mensaje CLLM. Los mensajes CLLM contienen un código de causa que indica el tipo y la gravedad del problema que se está informando. El dispositivo reacciona de manera diferente dependiendo del código de causa y la CIR configurada para cada PVC contenido en el mensaje CLLM. Cuando el dispositivo recibe un mensaje CLLM que indica:

- Una condición a corto plazo, y la CIR configurada para el PVC no es cero, el protocolo FR moderará la velocidad de transmisión para los PVC afectados por el porcentaje de decremento de IR configurado.
- Una condición a largo plazo, el protocolo FR establecerá la velocidad de transmisión para los PVC afectados en la velocidad mínima de información calculada.
- Una anomalía del recurso o del equipo o una acción de mantenimiento o si la CIR se ha configurado como cero, el protocolo FR continuará transmitiendo cualquier dato en cola para los PVC afectados pero no aceptará más paquetes de salida de los protocolos de capas superiores hasta que desaparezca la condición de congestión.

Cuando se ha recibido un mensaje CLLM para un PVC, si el dispositivo no recibe ningún mensaje CLLM o ninguna BECN durante el período del temporizador T_y o si se recibe una trama sin ninguna BECN, el dispositivo considerará que ha desaparecido la condición de congestión y devolverá gradualmente el PVC a sus velocidad de transmisión configurada. Si utiliza CLLM para controlar la congestión, no debe configurar el DLCI 1007 para ningún otro uso.

Congestión del circuito Frame Handler

Actuando como parte de la red de conmutación FR, los circuitos Frame Handler (FH) pueden realizar el control y la supervisión de la congestión de manera similar a los circuitos DTE. Cuando se ha habilitado la supervisión de CIR o de la congestión en una interfaz en la que se ha definido un circuito FH, éste y su circuito asociado trabajan conjuntamente para controlar la velocidad de datos a través del direccionador y para notificar a los circuitos DTE conectados cuando se produce una congestión. Entonces es responsabilidad del DTE reaccionar a las indicaciones de congestión de los circuitos FH.

Tenga en cuenta que a diferencia de los circuitos DTE, los circuitos FH no utilizan ninguna velocidad de información variable. La velocidad de envío para un circuito FH se establece en su valor configurado y no cambia nunca. De nuevo, es el DTE el que ha de cambiar su velocidad de envío como reacción a la congestión. El direccionador conservará los valores de bit BECN/FECN/DE en las tramas que está enviando, si el DTE u otro conmutador o direccionador ya habían establecido el bit en la vía de acceso; es decir, FH no desactivará los bits, pero puede activarlos.

El proceso de congestión para los PVC FH puede funcionar en una de tres modalidades: supervisión de CIR, supervisión de la congestión y sin supervisión. El tipo de supervisión utilizada para un PVC FH en particular se determina por lo que está habilitado en la interfaz de salida. Por ejemplo, si desea habilitar la supervisión de la velocidad de información de recepción para los PVC FH, debe habilitar la supervisión de CIR en la interfaz de salida del circuito. Aunque parezca algo confuso, lo más probable es que las interfaces en las que están definidos los PVC FH se configuren para el mismo tipo de supervisión.

Supervisión de CIR

Cuando habilite la supervisión CIR, se supervisarán las velocidades de datos de transmisión y de recepción para asegurarse de que se mantienen con los valores

Utilización de Frame Relay

configurados. Se utilizará un Tc de un segundo en la parte receptora sin tener en cuenta los valores de CIR y de Bc. Cuando FH procese una trama recibida, BECN se establecerá en la primera trama en cola para transmitir en dirección contraria (si existe una) y FECN se establecerá en la primera trama en cola para transmitir en la misma dirección (si existe una) si se cumple alguna de las condiciones siguientes:

- La recepción de la trama siguiente excede la velocidad de información de recepción. Utilizando un Tc de un segundo, se calcula la velocidad de información de recepción con $(Bc+Be)/(Bc/CIR)$.
- El dispositivo de entrada tiene pocos almacenamientos intermedios de recepción y la recepción de la trama siguiente excede el valor razonable para la interfaz.
- La recepción de la trama siguiente excede del 80% de la profundidad máxima de cola configurada.

La supervisión de CIR se configura con el mandato de configuración **enable cir-monitor** y está inhabilitada por omisión. Una trama se eliminará si se excede la CIR de recepción en un 10% o si se excede la profundidad máxima de cola. Si se ha de eliminar una trama, FR eliminará la primera trama que tenga el bit DE establecido y deba reenviarse. Si no se encuentra ninguna trama con el bit DE, se eliminará la trama recibida en lugar de reenviarse. La supervisión de CIR, cuando está habilitada, prevalece sobre la supervisión de la congestión. También puede habilitar o inhabilitar dinámicamente la supervisión de CIR utilizando los mandatos de consola (Talk 5) **enable cir-monitor** y **disable cir-monitor**.

Supervisión de la congestión

Cuando habilite la supervisión de la congestión, no se supervisarán las velocidades de datos para el circuito durante la transmisión o la recepción. Los bits BECN y FECN se enviarán bajo las condiciones siguientes:

- El dispositivo de entrada tiene poco almacenamiento intermedio de recepción y se excede el valor razonable para la interfaz.
- Se excede el 80% de la profundidad máxima de cola configurada.

Una trama se eliminará si la recepción de una trama de entrada excede la profundidad máxima de cola configurada. Si se ha de eliminar una trama, FR eliminará la primera trama que tenga el bit DE establecido y deba reenviarse. Si no se encuentra ninguna trama con el bit DE, se eliminará la trama recibida en lugar de reenviarse. La supervisión de la congestión es una característica opcional que puede establecerse por interfaz. La supervisión de la congestión está habilitada por omisión. Puede inhabilitarla con el mandato de configuración **disable congestion-monitor** y volverla a habilitar con el mandato **enable congestion-monitor**. También puede habilitar e inhabilitar dinámicamente la supervisión de la congestión utilizando los mandatos de consola (Talk 5) **enable congestion-monitor** y **disable congestion-monitor**.

Sin supervisión

Cuando no están habilitadas la supervisión de CIR ni la supervisión de la congestión, no se supervisarán las velocidades de datos de envío y de recepción y no se establecerán BECN ni FECN. El bit DE no se utilizará al determinar la trama que se ha de eliminar durante la congestión. En su lugar, si el dispositivo de entrada tiene pocos almacenamientos intermedios de recepción y se excede el valor razonable para la interfaz, o si la profundidad de cola de salida para el circuito FH alcanza 100, se eliminará la trama de entrada.

Reserva de ancho de banda en Frame Relay

Para obtener información sobre la reserva de ancho de banda en FR, consulte las secciones “Utilización de la reserva de ancho de banda y la puesta en cola con prioridad” y “Configuración y supervisión de la reserva de ancho de banda” de la publicación *Utilización y configuración de las características*.

El sistema de reserva de ancho de banda (BRS) debe configurarse para dar prioridad a los fragmentos de trama de datos si la fragmentación está habilitada en una interfaz. Consulte la sección “Fragmentación a través de una interfaz Frame Relay” para ver los detalles.

Fragmentación a través de una interfaz Frame Relay

Voice a través de Frame Relay (VoFR) es un método de transmisión de paquetes de voz a través de un circuito FR. Si piensa utilizar un circuito FR para transportar tanto tráfico en tiempo real (voz) como tráfico de datos, debe configurar ese circuito para fragmentar el tráfico de datos, especialmente si el enlace es relativamente lento, por ejemplo, 64 kbps. La fragmentación también es necesaria para los circuitos de interfaces que transportan tráfico de voz y para los circuitos de interfaces que no transportan tráfico de voz, pero que se comunican con interfaces que sí lo hacen.

Hay dos tipos de fragmentación, de extremo a extremo y de interfaz (o UNI/NNI). La fragmentación a nivel de interfaz no se ha implementado por ninguno de los principales proveedores de conmutadores FR y, por lo tanto, no está disponible en ningún proveedor de servicio FR. Por el acuerdo de implementación de FR, FRF.12, sólo se da soporte a la fragmentación de extremo a extremo para los PVC. Por lo tanto, se puede utilizar una interfaz con soporte de voz para soportar los PVC FR, pero no los SVC.

Puede configurar los tamaños de fragmentos. Los tamaños de fragmentos no se negocian ni se comunican entre interfaces y, por lo tanto, pueden ser diferentes para dos PVC interconectados. El tamaño de fragmento puede variar de un enlace o PVC a otro dependiendo de la velocidad de acceso del enlace, la CIR del PVC y si esta interfaz transporta realmente datos en tiempo real o se comunica con otro direccionador cuya interfaz transporta datos en tiempo real. Otros factores a tener en cuenta cuando se configura la fragmentación para la voz a través de frame relay son el tamaño de ráfaga confirmado, las clases de tráfico BRS y las profundidades de cola si está configurado BRS, el número de almacenamientos intermedios globales creados y el número de almacenamientos intermedios de recepción asignados a cada interfaz.

Debido a la actividad general asociada con la fragmentación, es mejor mantener el tamaño de fragmento lo más grande posible mientras se mantenga una alta calidad de las comunicaciones de datos en tiempo real.

Si un circuito transmite datos en tiempo real, debe configurar el Sistema de reserva de ancho de banda (BRS) además de la fragmentación de FR en esa interfaz y circuito. La habilitación de BRS puede proporcionar una prioridad más alta a los datos en tiempo real en relación a demás datos. Como resultado, los datos en tiempo real pueden interponerse entre los datos que se han fragmentado de modo que puede minimizarse el retardo de puesta en cola para los datos en tiempo real.

BRS sólo es necesario para los circuitos que realmente van a enviar datos en tiempo real y otros datos. Los otros circuitos de la interfaz, o los circuitos que se

Utilización de Frame Relay

comunican con interfaces que soportan datos en tiempo real, no necesitan específicamente el soporte de BRS para permitir la interposición.

Consulte el mandato **assign** en el capítulo “Configuración y supervisión de reserva de ancho de banda” de la publicación *Utilización y configuración de las características* para obtener más información acerca de la configuración de BRS.

Nota: Puede configurar la fragmentación para una interfaz o para un circuito (llamado también un PVC). Si configura la fragmentación para un PVC, debe utilizar los mandatos **add permanent-virtual-circuit** o **change permanent-virtual-circuit**. El ejemplo siguiente muestra el mandato **add permanent-virtual-circuit**:

```
FR 1 Config>add perm 18
Committed Information Rate (CIR) in bps[64000]?
Committed Burst Size (Bc)in bits [64000]? 4800
Excess Burst Size (Be) in bits [0]?
Assign circuit name : :? VoFRcircuit1
Is circuit required for interface operation [N]?
Enable circuit for voice forwarding [N]?
Do you want to have end-to-end fragmentation performed [N]? y
Fragment size (50 to 1000) [256]?
Fragmented packet reassembly timer (3 to 10 seconds) [256]?
```

Reenvío de voz a través de Frame Relay

El reenvío de voz a través de FR habilitará un direccionador con posibilidad de voz o uno sin posibilidad de voz para reenviar paquetes encapsulados FRF.11, es decir, paquetes de voz, entre los PVC FR sin utilizar ningún adaptador de voz nativo. Esto permitirá que un direccionador con posibilidad de voz multiplexe la voz y los datos a través del mismo circuito virtual en la red FR. Después, el direccionador de reenvío de voz direccionará los datos recibidos utilizando la pila de protocolos asociada al tráfico recibido y reenviará el tráfico de voz a otro PVC a través de la misma interfaz FR o de otra distinta. En una configuración típica, el tráfico de voz se reenvía a un dispositivo con posibilidad de voz conectado localmente.

Aunque sea una función parecida a DCE, el reenvío de paquetes de voz se realizará a través de circuitos virtuales definidos como DTE. El reenvío de voz sólo estará permitido para los PVC porque la voz a través de FR sólo está soportada para los PVC.

Un PVC que vaya a utilizarse para el reenvío de paquetes de voz debe habilitarse mediante la configuración para que lo haga. De hecho, deben definirse un par de PVC en interfaces FR que se suponen diferentes para que se reenvíen paquetes de voz entre sí. Cuando habilite un PVC para reenvío de voz, debe proporcionar el número de red y el DLCI del PVC al que el PVC debe reenviar los paquetes de voz. FR reenviará todos los paquetes de voz entre el par de PVC definidos para efectuar el reenvío de voz.

Sugerencias para configurar el 2216 para VoFR

Nota: El 2216 no origina tráfico de voz a través de FR, pero necesita una configuración especializada cuando se utiliza para reenviar tráfico de voz a través de FR.

Mediante la utilización de la multiplexión estadística, las redes Frame Relay proporcionan un medio excelente de transporte de datos, pero de algún modo representan un reto para la voz. El retardo del tránsito de cada paquete reenviado a través de una red Frame Relay es potencialmente diferente del paquete anterior.

Y aunque, las redes Frame Relay aseguran un secuencia adecuada de las tramas, no aseguran la entrega de todos los paquetes; el reintento y la recuperación se dejan para las capas superiores. El retardo de un paquete determinado se ve afectado en su mayor parte por la cantidad de tráfico adicional de la red presente cuando se reenvía el paquete. Existe la regla empírica general de que el tiempo de respuesta de ida y vuelta de un paquete de voz no debe exceder 250 milisegundos (ms); de lo contrario, los llamadores empezarán a sobreponerse entre sí. Para maximizar la calidad de las llamadas de voz, puede ajustarse la red del direccionador para minimizar el retardo del tránsito de los paquetes de voz.

Existen configuraciones que pueden utilizarse para soportar Voice a través de Frame Relay (VoFR) y cada una de ellas necesita consideraciones de ajuste diferentes. La fragmentación de Frame Relay juega un papel importante en la configuración si la voz se va a transportar a través de enlaces relativamente lentos (por ejemplo, de 64 kbps). También hay que tomar en consideración la CIR de Frame Relay y el tamaño de ráfaga confirmado, las clases de tráfico BRS y las profundidades de cola permitidas, el número global de almacenamientos intermedios creados y el número de almacenamientos intermedios de recepción asignados a cada interfaz.

Configuración de interfaces Frame Relay

La fragmentación es necesaria para todos los PVC de cualquier interfaz que vayan a utilizarse para la voz o cualquier otro dato de tiempo real, de prioridad alta. Hay dos tipos de fragmentación: de extremo a extremo y de interfaz (o UNI/NNI). La fragmentación a nivel de interfaz no se ha implementado por ninguno de los principales proveedores de conmutadores FR y, por lo tanto, ningún proveedor de servicio FR la tiene disponible. Por el acuerdo de implementación de Frame Relay Forum, FRF.12, sólo se da soporte a la fragmentación de extremo a extremo para los PVC. Por lo tanto, no debe utilizarse una interfaz con soporte de voz para dar soporte a los SVC FR.

La fragmentación es necesaria para minimizar la cantidad de retardo en la puesta en cola y la transmisión de paquetes de voz. La fragmentación debe utilizarse para todos los PVC que intercambian datos a través de una interfaz que soporta voz. Esto significa que un direccionador que no soporta la voz necesita efectuar la fragmentación si se comunica con otro direccionador que soporta la voz a través de la misma interfaz.

Los tamaños de fragmento pueden variar entre las interfaces FR dependiendo de la velocidad de acceso del enlace, la CIR del PVC y si esta interfaz transporta realmente voz o sólo se comunica con otro direccionador cuya interfaz transporta voz. Los tamaños de fragmento no se negocian ni se comunican entre las interfaces y, por lo tanto, pueden ser diferentes para dos PVC interconectados. Debido a la actividad general asociada con la fragmentación, es mejor mantener el tamaño de fragmento lo más grande posible a la vez que se mantienen comunicaciones de voz de alta calidad. Lo más importante que se ha de recordar es el límite de retardo de ida y vuelta de 250 milisegundos. Esto significa que cualquier componente dado de la red debe minimizar su porción de retardo y, sin embargo, maximizar su eficacia.

Cuando la voz y los datos se multiplexan a través del mismo PVC, el tamaño de ráfaga FR y el intervalo de ráfaga también son importantes en la reducción de la cantidad de retardo en que incurren los paquetes de voz. El intervalo de ráfaga, o T_c , se calcula por B_c/CIR (tamaño de ráfaga confirmado dividido por la CIR). Esto especifica la duración de la ráfaga. El tamaño de ráfaga es el número de bits que

Utilización de Frame Relay

el direccionador tiene configurado para enviar durante el Tc. Normalmente es Bc+Be, pero pueden ser más o menos, dependiendo de si está habilitada la supervisión de CIR o de la congestión y de si se ha recibido alguna indicación de congestión.

Por ejemplo, suponga que tiene una CIR de 64 kbps, un Bc de 64 kbs y un Be de 0; en este caso, el Tc es igual a un segundo. El direccionador permitirá una ráfaga de hasta 64 kbs en cualquier momento de ese período de 1 segundo. Si hay datos en cola para el circuito, los 64 kbs se enviarán directamente al principio del intervalo. El direccionador debe esperar ahora hasta el siguiente Tc, es decir, el siguiente segundo, antes de poder enviar más datos. Esto funciona bien para las transferencias de archivos y también para la voz sola porque la interfaz de voz envía los datos a la interfaz FR, a una velocidad fija, previsible, eliminando de este modo la ráfaga. Pero si el PVC se utiliza para transmitir tráfico de voz y de datos, la voz se pondría en cola hasta el máximo de un segundo en espera del siguiente intervalo Tc y este retardo es inaceptable.

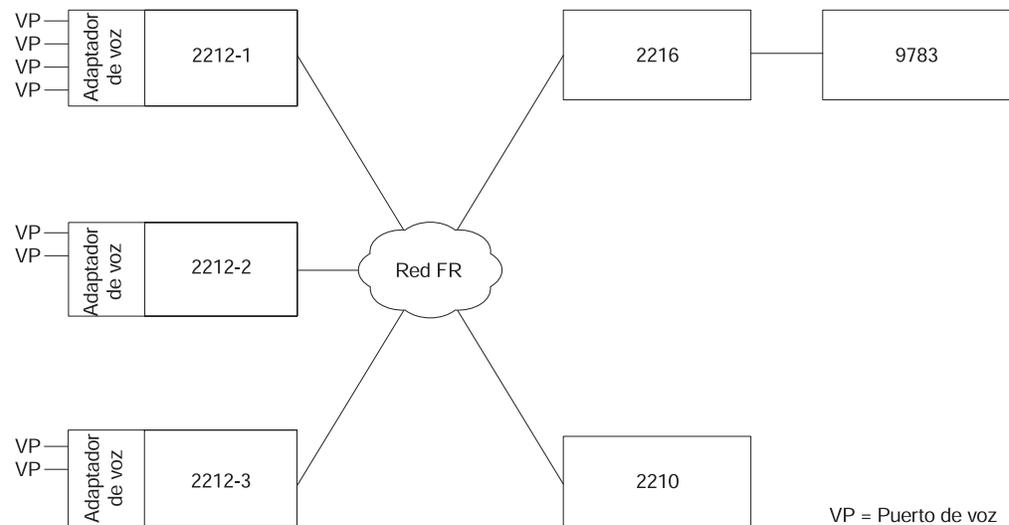


Figura 44. Ejemplo de configuración VoFR

Suponga que en esta configuración los 2212, los 2210 y los 2216 tienen un enlace de velocidad de acceso T1 cada uno con la red FR. Los 2212 y los 2210 tienen un solo PVC cada uno que conduce al 2216. Por lo tanto, el 2216 tiene un solo PVC a cada uno de los direccionadores. Se supone que los PVC para los demás direccionadores están en el mismo enlace. El 2216 tiene también un enlace FR de posterior a posterior con el IBM 9783 Voice FRAD a la velocidad T1.

La lista siguiente describe las consideraciones sobre la configuración que deben tomarse en cuenta al configurar los 2212:

- Si el PVC sólo va a transportar voz, será suficiente utilizar los valores por omisión para la interfaz de adaptador de voz y la interfaz FR. Sin embargo, si el PVC transporta voz y datos o sólo voz, es necesario tener en cuenta la cantidad de datos que cada llamada de voz genera para asegurarse de que hay ancho de banda disponible para transportar el tráfico. La cantidad de datos que un puerto de voz genera depende del codificador de voz y la velocidad configurada. Esta información puede reunirse en la Tabla 69 en la página 555.

Como otro ejemplo, suponga una velocidad de decodificador de 9,6 kbps. Los 9,6 kbs representan la cantidad de datos, menos las cabeceras, que se utilizarán para la llamada, suponiendo que no se suprime el silencio. Si no se utiliza el

Utilización de Frame Relay

empaquetamiento de tramas, el ancho de banda real utilizado es 12 800 bps por llamada. Por lo tanto un PVC con una CIR de 64 kbps sólo puede transportar cuatro llamadas de voz a la velocidad de 9,6 kbps. Un PVC que sólo transporta voz no necesita tener la posibilidad de fragmentación; sólo transporta voz y los paquetes de voz no se fragmentan.

Tabla 69. Datos generados por un puerto de voz

Codificador de voz	Bits por segundo con actividad general	Bytes por trama	Paquetes por segundo
4800	8000	15	67
7500	10 670	20	67
8000	10 400	26	50
9600	12 800	25	67
16 000	19 200	36	67
32 000	35 200	66	67

- Todos los PVC que no transportan voz, pero que están en la misma interfaz que un PVC que transporta voz, deben habilitarse para la fragmentación. El tamaño de fragmentación depende de la velocidad de acceso, el número de puertos de voz soportados en la interfaz y la cantidad de retardo que puede tolerar en la conexión de voz. Por ejemplo, con el codificador de voz y velocidad facilitados arriba, el módulo de voz portátil (PVM), es decir, el adaptador de voz, transmitirá una trama de voz cada 15 ms. Lo mejor es minimizar el retardo de puesta en cola para cada paquete de voz, pero puede tolerarse algo de puesta en cola. Si supone que un retardo de 30 ms es tolerable, el tamaño de fragmento del PVC sin posibilidad de voz de una línea de 64 kbps debe ser aproximadamente de 240 ($64\,000 * 0,030$) bytes. Si el PVC está en una línea T1, puede que no sea necesaria la fragmentación si el retardo de 30 ms es aceptable ($1\,544\,000 * 0,030 = 5790$ bytes).
- Los PVC que transportan voz y datos necesitan un ajuste más preciso. Es cuando no sólo debe ajustar el tamaño de fragmento, sino también la CIR y el tamaño de ráfaga para acomodar la mezcla de voz y de datos. De nuevo, debe tomar en consideración la velocidad de acceso, el número de llamadas y el codificador de voz y la velocidad.
- Por ejemplo, suponga que el 2212-1 que aparece en la Figura 44 en la página 554 tiene cuatro puertos de voz que pueden estar activos a la vez. En la prueba, se ha encontrado que era tolerable un retardo de 60 ms de la voz en la interfaz FR. Esto significa que el intervalo de ráfaga del PVC, T_c , debe establecerse en 60 ms. El T_c no se puede configurar directamente, pero, tal como se indica antes, se determina por B_c/CIR . Si la CIR es de 64 kbps, el establecimiento del B_c en 3840 bits da como resultado un T_c de 60 ms. B_c se establece en cero; B_c puede establecerse en un número mayor que cero si la red RF va a permitir que el PVC realice ráfagas por encima de su CIR. Esto significa que el PVC puede enviar 3840 bits (480 bytes) por 60 ms. Si hace esto, conseguirá una velocidad de envío de 64 kbps ($60\text{ ms} = ,06$ segundos; $3840/,06 = 64\,000$ bps). Las cuatro llamadas de voz generarán una trama de 25 bytes cada 15 ms cada una. Esto significa que en un intervalo de 60 ms, los puertos de voz enviarán 400 bytes ($25\text{ bytes} * 4\text{ tramas} * 4\text{ llamadas}$) por intervalo. Esto da 80 bytes por T_c para enviar datos. Por lo tanto, el tamaño de

Utilización de Frame Relay

fragmento debe establecerse en 74 (80 - 6 bytes de actividad general). Para que se acepte el Tc para un PVC, debe habilitar la supervisión de CIR para esta interfaz.

Como otro ejemplo, suponga que sólo tiene dos llamadas de voz a través del mismo PVC anterior. El Tc debe ser todavía 60 ms, lo que significa que el Bc debe seguir estableciéndose en 3840. Sin embargo, el tamaño de fragmento cambiará, ya que ahora se puede enviar un fragmento mayor en el mismo intervalo Tc con los paquetes de voz. En este caso, el tamaño de fragmento debe establecerse en 274 bytes ($480 - (25 * 4 * 2) - 6$).

- FR soporta un Tc mínimo de 30 ms. Los paquetes de voz son pequeños por norma, por lo tanto si se reduce el Tc no afectará al rendimiento del tráfico de voz. Sin embargo, la utilización de un Tc pequeño fuerza a que el tamaño de fragmento sea menor y los tamaños de fragmentos pequeños no son eficaces para el ancho de banda, la utilización de procesador y el uso de almacenamiento intermedio global. Es mejor buscar el Tc mayor y, por lo tanto, el tamaño de fragmento más grande que se pueda utilizar para mantener una buena calidad de voz.

Las consideraciones para ajustar el 2216 son las mismas que para el 2212 porque realiza el reenvío de voz entre los PVM de los 2212 y el IBM 9783 Voice FRAD.

El 2210 no envía ningún tráfico de voz; sin embargo, se comunica con la interfaz 2216 que envía tráfico de voz. En este caso, el 2210 no necesita ningún ajuste especial que no sea la habilitación del PVC para la fragmentación. El PVC de 2210 no necesita realmente fragmentar sus paquetes de salida, pero debe estar habilitada la fragmentación para permitirle recibir los paquetes fragmentados. Por lo tanto, el tamaño de fragmentación para este PVC debe establecerse en la MTU para la interfaz o 8190, que es la MTU máxima para una interfaz FR. En cualquier caso, el 2210 no fragmentará las tramas que envíe pero volverá a ensamblar las que el 2216 le ha enviado.

Dependiendo del número de llamadas de voz soportadas y las velocidades de acceso, puede que también necesite aumentar el número de almacenamientos intermedios de entrada por interfaz. Los almacenamientos intermedios de entrada son necesarios debido a los retardos de cola causados cuando FR ejecuta los temporizadores de ráfagas. Lo que ocurre generalmente en una línea T1 es que el PVC rellenará su tamaño de ráfaga inmediatamente y, después, se detendrá temporalmente por el Tc (60 ms en el ejemplo anterior) antes de volver a realizar un envío. Esto significa que el circuito pondrá en cola 60 ms de tramas de voz antes de volver a enviar. Los mecanismos de control del flujo del direccionador pueden provocar que se eliminen paquetes de voz, de modo que afecte a la transmisión antes de que el usuario se dé cuenta de que existe un problema en la calidad de voz. Los problemas de transmisión vienen indicados porque el adaptador de voz deja en suspenso las llamadas de voz o porque no se puede iniciar una llamada de voz incluso cuando hay ancho de banda disponible.

En estos casos, puede que sea necesario aumentar el número de almacenamientos intermedios de recepción en las interfaces FR y de adaptador de voz. La mejor manera de supervisar las tramas eliminadas es utilizando los mandatos **error** y **interface** de Talk 5. Si se detectan eliminaciones de entradas en los adaptadores de voz o que faltan tramas en las interfaces de voz o FR, debe aumentarse el número de almacenamientos intermedios de recepción. Sin embargo, las eliminaciones de entrada y de salida en interfaces FR pueden ser normales y aceptables si alguno de los circuitos FR se está cargando

excesivamente con datos, por ejemplo, cuando el 2216 intenta transferir un archivo grande mientras hay cuatro llamadas de voz activas.

Configuración del BRS

Es necesario configurar el BRS en todas las interfaces que soportan voz y datos. Se puede utilizar el BRS para controlar el número de almacenamientos intermedios que se pueden poner en cola para un circuito en particular y la prioridad que se ha dado a los datos que se ponen en cola.

Las profundidades de cola mínima y máxima se configuran por circuito en el nivel del BRS. Estas profundidades de cola se aplican a cada una de las cuatro colas de cada clase de tráfico que el BRS mantiene. La profundidad de cola mínima determina cuándo el BRS desechará las tramas de entrada cuando el dispositivo de entrada tenga pocos almacenamientos intermedios de recepción. Tener pocos almacenamientos intermedios de recepción significa que el dispositivo de entrada tiene x o menos almacenamientos intermedios disponibles para recibir datos, donde x es igual a la cuenta de *poco*, tal como lo visualiza el mandato **queue** de talk 5.

El BRS devolverá el almacenamiento intermedio al dispositivo de entrada si éste tiene pocos almacenamientos intermedios de entrada y si, actualmente, el número de almacenamientos intermedios de la cola a la que se añadiría la trama de entrada es igual o mayor que la profundidad de cola mínima y menor que la profundidad de cola máxima. Sin tener en cuenta si el dispositivo de entrada tiene pocos almacenamientos intermedios o no, la profundidad de cola máxima determina el número máximo de almacenamientos intermedios que se pondrán en la cola de prioridad. Los valores de profundidad de cola mínima y máxima deben aumentarse junto con el número de almacenamientos intermedios de recepción por interfaz cuando se detecten eliminaciones de entradas. Las eliminaciones de entradas se visualizan por interfaz utilizando el mandato **statistics** de talk 5.

Después, tome en consideración las clases de tráfico que se utilizan para dar preferencia de ancho de banda al tráfico de voz. Las definiciones de clase de tráfico sólo necesitan definirse si se van a multiplexar la voz y los datos en el mismo PVC, porque las clases de tráfico no interfieren ni se interrumpen entre sí en los circuitos. Normalmente, debe darse prioridad a la voz a través de cualquier otro tipo de tráfico para un PVC. Para dar prioridad a la voz, tiene las dos opciones siguientes:

1. Cree una clase de tráfico con nombre. Esto da como resultado dos clases de tráfico, porque siempre se crea la clase LOCAL y se utiliza para el tráfico generado internamente por el direccionador, es decir, RIP y PING. Asigne todos los protocolos a la clase de tráfico que ha creado y asigne la prioridad más alta de esa clase al tráfico de voz (P_VOFR) para que se envíe primero, antes de todos los demás protocolos. Los datos de protocolo de prioridad superior dentro de una clase siempre se envían antes que los datos de prioridad inferior. Los datos de protocolo asignados a la misma prioridad dentro de una clase se envían por orden FIFO. Un problema potencial es que si se produce una congestión, el tráfico de voz siempre se envía primero y es posible que haya otros protocolos que nunca se envíen. Esta condición se llama *rendición por necesidad*.
2. Cree una clase de tráfico superior y asigne voz a la misma. Asigne los demás protocolos a diferentes clases de tráfico, asignando porcentajes de ancho de banda a cada clase, según proceda. La clase superior no tiene un porcentaje de ancho de banda asignado a la misma. El tráfico en la cola de esta clase se enviará antes que los datos de cualquier otra clase de tráfico. La utilización de

Utilización de Frame Relay

múltiples clases de tráfico le permite dar preferencia a protocolos de prioridad alta sin que los protocolos de prioridad menor se rindan por necesidad.

Las clases de circuito BRS también pueden ser necesarias para dar preferencia de ancho de banda a los PVC que transportan voz sobre los que sólo transportan datos. Las definiciones de clase de circuito sólo son necesarias cuando la suma de las CIR para los circuitos de la interfaz excede la velocidad de acceso del enlace. Si la CIR total no excede la velocidad de acceso, no se utilizan los porcentajes de ancho de banda asignados a las clases de circuitos porque la función de forma de tráfico FR (es decir, la supervisión de CIR) prevalecerá sobre las asignaciones de ancho de banda de clase de circuito. Si la CIR total excede la velocidad de acceso, las clases de circuito deben definirse de manera que los PVC que transportan voz tengan porcentajes de ancho de banda superiores a los que sólo transportan datos.

Visualización del indicador de configuración de Frame Relay

Para acceder al entorno de configuración FR:

1. En el indicador OPCON (*), escriba **talk 6**.
2. En el indicador de configuración (Config>), entre el mandato **list devices** para ver una lista de interfaces configuradas en el direccionador.
3. Entre el mandato **network** para visualizar el indicador de configuración FR. El número de red es el número de la interfaz FR.

```
Config>network
Network number [0]? 2
Frame Relay user configuration
FR 2 Config>
```

4. En el indicador de configuración de interfaz FR (en el ejemplo, FR 2 Config>), utilice los mandatos explicados en este capítulo para configurar los parámetros FR.

Procedimiento de la configuración básica de Frame Relay

Esta sección indica los pasos de la configuración mínima que es necesaria para activar y ejecutar el protocolo FR. Si desea más información de configuración y una explicación, consulte los mandatos de configuración descritos en este capítulo.

Nota: Debe reiniciar el direccionador para que los cambios de la nueva configuración surtan efecto.

- **Seleccione la gestión FR.** El protocolo Local Management Interface (LMI) FR toma por omisión ANSI. Tiene la opción de conectar con una red utilizando la gestión Interim LMI (REV1), ANSI T1.617 Anexo D o la gestión ITU-T/CCITT Q.933 Anexo A. Utilice los mandatos **enable** y **set** para habilitar y establecer la gestión necesaria.
- **Añada un PVC.** Añada cualquier PVC necesario si la gestión FR está inhabilitada o si los circuitos huérfanos están inhabilitados. Si desea realizar una función de puente a través de un PVC FR o si desea ejecutar APPN a través de un PVC FR, también debe configurar ese PVC. Utilice el mandato **add permanent-virtual-circuit**.
- **Configure las direcciones de destino FR.** Si está ejecutando un protocolo como, por ejemplo, IP o IPX a través de la interfaz FR y está interconectando con dispositivos que no dan soporte a Address Resolution Protocol (ARP) ni a Inverse ARP en FR, utilice el mandato **add protocol-address** para añadir el protocolo estático y la correlación de direcciones.
- **Configure la reserva de ancho de banda en Frame Relay.** Además de la configuración FR básica, la cual debe efectuarse, también puede configurar la

Reserva de ancho de banda (una característica opcional) en FR. Para obtener información sobre la configuración de la Reserva de ancho de banda, consulte la sección “Utilización de la reserva de ancho de banda y la puesta en cola con prioridad” de la publicación *Utilización y configuración de las características*.

- **Configure la Elegibilidad para eliminar.** Puede configurar el control de congestión de Elegibilidad para eliminar (DE) utilizando la Reserva de ancho de banda. Para obtener información acerca de la configuración de la Elegibilidad para eliminar, consulte la sección “Utilización de la reserva de ancho de banda y la puesta en cola con prioridad” de la publicación *Utilización y configuración de las características*.
- **Configure la compresión de datos.** Puede configurar la compresión de datos para FR. Para obtener información sobre la configuración de la compresión de datos, consulte la sección “Configuración y supervisión de compresión de datos” de la publicación *Utilización y configuración de las características*.
- **Configure el cifrado de datos.** Puede configurar el cifrado de datos para FR. Para obtener información sobre la configuración del cifrado de datos, consulte la sección “Utilización y configuración de encriptación de datos” de la publicación *Utilización y configuración de las características*.

Habilitación de la gestión de PVC en Frame Relay

Hay tres opciones de gestión bajo Frame Relay:

- Interim Local Management Interface Revisión 1
- Gestión ANSI T1.617 Anexo D
- Gestión ITU-T/CCITT Q.933 Anexo A.

FR toma por omisión la habilitación de ANSI. Si desea cambiar los tipos de gestión o si desea volver a habilitar la gestión ANSI, utilice el procedimiento siguiente. La habilitación de la gestión a través de FR es un proceso de dos pasos:

1. Entre el mandato **enable lmi** en el indicador FR Config> para habilitar la actividad de la gestión.
2. Entre el mandato **set lmi-type** para seleccionar el tipo de gestión para la interfaz.

Consulte la Tabla 70 para ver los detalles de los tipos de gestión disponibles mediante la utilización del mandato **set**.

Nota: El valor por omisión del tipo de red LMI es UNI (interfaz de usuario a red). Esta es la configuración más común necesaria cuando se conecta el dispositivo a una red FR pública. Si es necesaria una interfaz NUI (red a usuario) o NNI (red a red), utilice el mandato **set LMI-network-type** para configurar la interfaz adecuadamente.

Después de la tabla, aparece un ejemplo de cómo establecer estos tipos de gestión. Consulte también las secciones de los mandatos **enable** y **set** de este capítulo para obtener más información.

Tabla 70. Opciones de gestión de Frame Relay

Mandato	Opciones	Descripción
set	lmi-type rev1	Cumple con LMI Revision 1 (especificación de interfaz Frame Relay Stratacom s)
set	lmi-type ansi	Cumple con ANSI T1.617 RDSI-DSS1-Signalling Specification for Frame Relay Bearer Service (known as Annex D)

Utilización de Frame Relay

Tabla 70. Opciones de gestión de Frame Relay (continuación)

Mandato	Opciones	Descripción
set	lmi-type ccitt	Cumple con el Anexo A de ITU-T/CCITT Recommendation Q.933 - DSS1 Signalling Specification for Frame Mode Basic Call Control.

Ejemplo:

```
enable lmi
set lmi-type ansi
```

Habilitación de la gestión de SVC en Frame Relay

La gestión SVC FR se habilita automáticamente cuando se habilitan los SVC.

Capítulo 42. Configuración y supervisión de interfaces Frame Relay

Este capítulo describe los mandatos de configuración y operativos de Frame Relay e incluye las secciones siguientes:

- “Mandatos de configuración Frame Relay”
- “Acceso al indicador de supervisión de Frame Relay” en la página 600
- “Mandatos de supervisión Frame Relay” en la página 600
- “Interfaces Frame Relay y mandato interface de GWCON” en la página 615
- “Soporte para la reconfiguración dinámica de Frame Relay” en la página 617

Notas:

1. Para obtener información acerca de la supervisión de la reserva de ancho de banda en Frame Relay, consulte la sección “Configuración y supervisión de reserva de ancho de banda” de la publicación *Utilización y configuración de las características*.
2. Se utiliza el mandato **add dev fr** del mandato `Config>` de Talk 6 para crear las subinterfaces de Frame Relay. Consulte la sección “Subinterfaces para Frame Relay” en la página 533 para obtener más información.

Mandatos de configuración Frame Relay

Esta sección describe los mandatos de configuración Frame Relay. Entre todos los mandatos en el indicador `Frame Relay n>`, donde *n* representa el número de interfaz. Debe reiniciar el direccionador para que los cambios en la nueva configuración surtan efecto. La Tabla 71 muestra los mandatos. Para acceder al indicador `Frame Relay n>`, efectúe los pasos siguientes:

1. En el indicador `OPCON (*)`, escriba **talk 5**.
2. En el indicador `GWCON (+)`, entre el mandato **interface** para ver una lista de las interfaces configuradas en el direccionador.
3. Seleccione la interfaz Frame Relay que configurará.
4. Escriba **exit**.
5. En el indicador `OPCON (*)`, escriba **talk 6**.
6. En el indicador `Config>`, entre el mandato **network** seguido del número de red de la interfaz frame relay. Por ejemplo:

```
Config> net 2
Frame Relay user configuration
FR 2 Config>
```

Tabla 71. Resumen de los mandatos de configuración de Frame Relay

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página 10.
Add	Añade los PVC, los grupos de PVC necesarios, los SVC y las direcciones de protocolo de destino a la interfaz Frame Relay.
Change	Modifica un PVC, un SVC o un grupo de PVC necesario definido previamente por el mandato add .
Disable	Inhabilita cualquier característica habilitada de Frame Relay.
Enable	Habilita las características de Frame Relay como, por ejemplo, la supervisión de circuitos, las opciones de gestión, la multidifusión, la difusión de protocolos, la fragmentación y los huérfanos.

Configuración de interfaces Frame Relay (Talk 6)

Tabla 71. Resumen de los mandatos de configuración de Frame Relay (continuación)

Mandato	Función
List	Visualiza la configuración actual de la LMI, los PVC, los grupos de PVC necesarios, los SVC, la información HDLC y las direcciones de protocolo.
LLC	Configura los parámetros LLC en la interfaz Frame Relay. Estos parámetros LLC son necesarios al ejecutar APPN en la interfaz Frame Relay.
Remove	Suprime cualquier PVC, SVC o grupo de PVC necesario (si está vacío) o dirección de protocolo que se ha añadido previamente.
Set	Configura las opciones y los parámetros de la gestión de Frame Relay (parámetro N1, parámetro N2, parámetro N3, parámetro P1 y parámetro T1). Configura los parámetros de la capa física para interfaces serie FR. Establece el tamaño máximo de trama.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página 11.

Nota: En esta sección, los términos *número de circuito* y *PVC* son sinónimos del término *DLCI* (Identificador de circuito de enlace de datos).

Add

Utilice el mandato **add** para añadir un circuito, un grupo PVC necesario o una dirección de protocolo de destino soportados por la interfaz Frame Relay.

Sintaxis:

```
add                frame-handler-pvc  
                    permanent-virtual-circuit . . .  
                    protocol-address . . .  
                    pvc-group . . .  
                    switched-virtual-circuit . . .
```

frame-handler-pvc

Añade el soporte de manejador de tramas para permitir el tráfico direccionado, de puente, de voz y DCE a través de la misma interfaz.

Ejemplo:

```
FR 4 config> add frame-handler-pvc  
Circuit Number [16]?  
Committed Information Rate (CIR) in bps [64000]?  
Committed Burst Size (Bc) in bits [64000]?  
Excess Burst Size (Be) in bits [0]?  
Assign Circuit name []?  
Network number of FH partner PVC [0]?  
Circuit number of FH partner PVC [16]?  
Maximum outbound queue depth (in number of packets) [10]? 1
```

Circuit Number

Indica el número de circuito para este PVC.

Valores válidos: De 16 a 1007. El número de circuito debe ser exclusivo con respecto a los demás PVC y PVC FH de esta interfaz y todas las subinterfaces asociadas.

Committed Information Rate

Indica la velocidad de información confirmada (CIR). La CIR puede tener un valor en el rango de 300 bps a 2 048 000 bps. Para obtener más información, consulte la sección “Velocidad de

Configuración de interfaces Frame Relay (Talk 6)

información confirmada (CIR)” en la página 543. El máximo es el valor de la CIR por omisión configurada para la interfaz.

Nota: El valor por omisión se determina de acuerdo a los valores por omisión de la CIR establecidos a nivel de interfaz.

Committed Burst Size

La cantidad máxima de datos en bits que la red acuerda entregar durante un intervalo de medición igual al tamaño de ráfaga confirmado (Bc) / CIR segundos. El rango es de 300 a 2 048 000 bits. El valor máximo es el valor por omisión de la ráfaga confirmada configurado para la interfaz. Consulte la sección “Tamaño de ráfaga confirmado (Bc)” en la página 544 para obtener más información.

Nota: El valor por omisión se determina de acuerdo a los valores por omisión de Bc establecidos a nivel de interfaz.

Excess Burst Size

La cantidad máxima de datos no confirmados en bits que exceden del tamaño de ráfaga confirmado que la red intenta entregar durante un intervalo de medición igual a (Tamaño de ráfaga confirmado/CIR) segundos. El rango es de 0 a 2 048 000 bits. El valor máximo es el valor configurado para el tamaño de exceso de ráfaga para la interfaz. Para obtener información adicional, consulte la sección “Tamaño de exceso de ráfaga (Be)” en la página 544.

Nota: El valor por omisión se determina de acuerdo a los valores por omisión de Be establecidos a nivel de interfaz.

Assign Circuit Name

Indica la serie ASCII que se asigna para describir el PVC. El valor por omisión es *sin asignar*.

Network number of FH partner PVC

Especifica el número de red del PVC de manejador de tramas asociado.

Circuit number of FH partner PVC

Especifica el número de circuito del PVC de manejador de tramas asociado.

Maximum outgoing queue depth

Especifica el número máximo de tramas que pueden ponerse en la cola de salida para el PVC de manejador de tramas y se utiliza durante el proceso de la congestión.

Valores válidos: De 5 a 100

Valor por omisión: 10

permanent-virtual-circuit

Añade un PVC a la interfaz Frame Relay más allá del rango reservado de 0 a 15. El número máximo de PVC que pueden añadirse es 992 aproximadamente, pero el número real de PVC que la interfaz puede soportar depende de estas condiciones:

- La productividad necesaria para cada PVC
- La velocidad de línea
- Los tipos de protocolo que se ejecutan en la interfaz

Configuración de interfaces Frame Relay (Talk 6)

- El número de elementos de información de PVC de la interfaz de gestión local que caben en el tamaño máximo

Ejemplo:

```
add permanent-virtual-circuit
Circuit Number [16]?
Committed Information Rate (CIR) in bps [64000]?
Committed Burst Size (Bc) in bits [64000]?
Excess Burst Size (Be) in bits [0]?
Assign Circuit name []?
Is circuit required for interface operation [N]? y
Does the circuit belong to a required PVC group [N]? y
What is the group name []? group1
Do you want to have data compression performed [Y]?
Do you want to have end-to-end fragmentation performed [Y]?
Fragment size (50 to 8190) [256]?
Fragmented packet reassembly timer (3 to 10 seconds) [3]?
Enable circuit for voice forwarding [N]? y
Network number of voice forwarding PVC [0]?
Circuit number of voice forwarding PVC [16]?
Do you want to have data encryption performed [N]? y
Should the encryption algorithm be CDMF (CDMF) or triple-DES (3DES) [CDMF]?
Data encryption requires a key that is 16 hexadecimal characters long for CDMF,
48 hexadecimal characters long for 3DES.
```

You will be asked to enter the key twice for security reasons

Please enter the key for the first time now

A valid encryption key has been entered

Please confirm the key by entering it again

The encryption keys match - the key has been accepted

Circuit Number

Indica el número de circuito para este PVC.

Valores válidos: De 16 a 1007. El número de circuito debe ser exclusivo con respecto a los demás PVC y PVC FH de esta interfaz y todas las subinterfaces asociadas.

Committed Information Rate

Indica la velocidad de información confirmada (CIR). La CIR puede ser 0 o un valor en el rango de 300 bps a 2 048 000bps. Para obtener más información, consulte la sección “Velocidad de información confirmada (CIR)” en la página 543. El máximo es el valor de la CIR por omisión configurada para la interfaz.

Nota: El valor por omisión se determina de acuerdo a los valores por omisión de la CIR establecidos a nivel de interfaz.

Committed Burst Size

La cantidad máxima de datos en bits que la red acuerda entregar durante un intervalo de medición igual al tamaño de ráfaga confirmado (Bc) / CIR segundos. El rango es de 300 a 2 048 000 bits. El valor máximo es el valor por omisión de la ráfaga confirmada configurado para la interfaz. Para obtener información adicional, consulte la sección “Tamaño de ráfaga confirmado (Bc)” en la página 544.

Notas:

1. El valor por omisión se determina de acuerdo a los valores por omisión de Bc establecidos a nivel de interfaz.
2. No se soporta la CIR configurada como 0 para los PVC FH.

Excess Burst Size

La cantidad máxima de datos no confirmados en bits que exceden del tamaño de ráfaga confirmado que la red intenta entregar durante un intervalo de medición igual a (Tamaño de ráfaga

Configuración de interfaces Frame Relay (Talk 6)

confirmado/CIR) segundos. El rango es de 0 a 2 048 000 bits. El valor máximo es el valor configurado para el tamaño de exceso de ráfaga para la interfaz. Para obtener información adicional, consulte la sección "Tamaño de exceso de ráfaga (Be)" en la página 544.

Nota: El valor por omisión se determina de acuerdo con los valores por omisión de Be establecidos a nivel de interfaz.

Assign Circuit Name

Indica la serie ASCII que se asigna para describir el PVC. El valor por omisión es *sin asignar*.

Is the circuit required for operation?

Especifique **Y** o **N** para indicar si el circuito es necesario para el funcionamiento de la interfaz.

Does the circuit belong to a required PVC group?

Esta solicitud sólo se visualiza para los circuitos que son necesarios. Especifique **Y** o **N** para indicar si el circuito debe pertenecer a un grupo de PVC necesario.

What is the group name?

Le permite especificar el nombre del grupo de PVC necesario cuando el PVC se define como perteneciente a un grupo necesario. Entre un signo de interrogación (?) para ver una lista de los grupos definidos actualmente.

Do you want to have compression performed?

Le permite especificar si el circuito comprimirá o no los paquetes de datos. Esta pregunta sólo aparece si la compresión está habilitada en la interfaz.

Nota: Si habilita la compresión en un PVC y excede el límite del circuito de compresión de la interfaz, recibirá un mensaje. Si es posible, se efectuará la compresión en el circuito, es decir, si no se ha excedido el límite de compresión activo cuando se activa el circuito. El límite de compresión incluye el número de contextos de compresión asignados a los SVC así como a los PVC.

Enable circuit for voice forwarding?

Le permite especificar si el circuito reenviará o no paquetes de voz. Si especifica **Y** (sí), debe especificar el número de red y de circuito del PVC al que este PVC reenviará las tramas de voz.

Do you want to have end-to-end fragmentation performed?

Le permite especificar si el circuito efectuará la fragmentación o no en todo el circuito. Esta pregunta sólo aparece si se ha habilitado la fragmentación de extremo a extremo en la interfaz. Si está habilitada la fragmentación UNI/NNI, se habilita automáticamente la fragmentación en todos los circuitos de esta interfaz y esta pregunta no aparece.

Cuando especifique los valores de tamaño de fragmento y de temporizador de reensamblaje, puede alterar temporalmente los valores de tamaño de fragmento de extremo a extremo y de temporizador de reensamblaje para esta interfaz.

Do you want to have data encryption performed?

Le permite especificar si el circuito cifrará o no los paquetes de

Configuración de interfaces Frame Relay (Talk 6)

datos. Esta pregunta sólo aparece si el cifrado está habilitado en la interfaz. Las solicitudes de la clave de cifrado y el algoritmo sólo aparecen si responde **Y** (sí) a esta pregunta.

Specifying the Encryption Key: Debe especificar el valor de clave de cifrado en caracteres hexadecimales.

Valores válidos: 16 caracteres hexadecimales para CDMF, 48 caracteres hexadecimales para 3DES

Nota: El soporte de cifrado es opcional y debe añadirse a la carga de software utilizando el mandato **load add**. Consulte la sección "Load" en la página 101.

protocol-address

Este mandato añade direcciones de protocolo de destino (nombre-protocolo) configuradas estáticamente a la interfaz Frame Relay. Las direcciones de protocolo de destino configuradas estáticamente son útiles si Inverse ARP o ARP no aparecen como opciones o por otras razones como, por ejemplo, por seguridad. La adición del nombre de protocolo y las correlaciones de direcciones (ARP estático) es menos eficaz que Inverse ARP o ARP.

- Inverse ARP es el método eficaz, preferido porque correlaciona direcciones dinámicamente sin difusiones.
- Se recomienda ARP si Inverse ARP no aparece como opción. Es menos eficaz que Inverse ARP porque utiliza la difusión de direcciones y las correlaciones se vuelven a reconocer a intervalos regulares.

Este parámetro le solicita una información diferente dependiendo del tipo de protocolo que esté añadiendo.

Ejemplo:

```
add protocol-address  
Protocol name or number [IP]?
```

Protocolo IP:

```
IP Address [0.0.0.0]?  
Circuit Number or name[16]?
```

Protocolo IPX:

```
Host Number (in hex)[]?  
Circuit Number or name[16]?
```

Protocolo AppleTalk Phase 2:

```
Network Number (1-65279) []?  
Node Number (1-253) []?  
Circuit Number or name[16]?
```

Protocolo DN:

```
Node address [0.0]?  
Circuit Number or name[16]?
```

Protocol name or number

Define el nombre o número del protocolo que está añadiendo. Si especifica un protocolo no soportado, el sistema le enviará un mensaje de error:

```
Unknown protocol name, try again
```

Por ejemplo, puede haber especificado incorrectamente uno de los elementos siguientes:

Configuración de interfaces Frame Relay (Talk 6)

Prot#	Name
0	IP
4	DN
7	IPX
22	AP2

Para ver una lista de tipos de protocolos soportados escriba ? en la solicitud Protocol name or number [IP]? .

IP Address

Define la dirección Internet de 32 bits en notación decimal con puntos del sistema principal IP remoto.

Host Number

Define la dirección de nodo IPX de 48 bits del sistema principal IPX remoto.

Network Number

Define el número de red AppleTalk Phase 2 del sistema principal AppleTalk remoto.

Node Number

Define el número de nodo de la interfaz conectada al sistema principal AppleTalk remoto.

Node address

Define la dirección de nodo DECnet del sistema principal DECnet remoto. Configure la dirección de nodo con el formato *x.y*, donde *x* es una dirección de área de 6 bits e *y* es un número de nodo de 10 bits.

Circuit Number or name

Define el PVC por su DLCI o nombre o el SVC por su nombre con el que esta dirección de protocolo remota está conectada.

pvc-group *nombregrupo*

Añade un nombre de grupo de PVC necesario.

Nota: Los SVC pueden no pertenecer a un grupo de PVC necesario.

switched-virtual-circuit

Añade un circuito virtual conmutado (SVC). El SVC actuará de forma similar a un PVC excepto en que la red FR asignará dinámicamente el ancho de banda del SVC únicamente cuando el SVC esté activo. El número de SVC que se pueden añadir es similar al número de PVC que pueden añadirse en que depende de la productividad necesaria para cada circuito, la velocidad de línea, etc. Sin embargo, puesto que el ancho de banda de un SVC sólo está reservado cuando el SVC está activo, puede que sea posible soportar más SVC que PVC en una interfaz.

```
FR 4 Config>add switched-virtual-circuit
Circuit name []? svc01
Remote party number []? 12345
Remote party number numbering plan (E.164 or X.121) [E.164]?
Remote party number type (Unknown or International) [International]?
Remote party subaddress in hexadecimal []? 01
Remote party subaddress format (private or NSAP) [private]?
Requested outgoing Committed Information Rate (CIR) in bps [64000]?
Minimum acceptable outgoing Committed Information Rate (CIR) in bps [64000]?
Requested incoming Committed Information Rate (CIR) in bps [64000]?
Minimum acceptable incoming Committed Information Rate (CIR) in bps [64000]?
Requested outgoing Committed Burst size (Bc) in bits [64000]?
Requested incoming Committed Burst size (Bc) in bits [64000]?
Requested outgoing Excess Burst size (Be) in bits [0]?
Requested incoming Excess Burst size (Be) in bits [0]?
Idle timer in seconds [60]?
```

Configuración de interfaces Frame Relay (Talk 6)

Establish circuit to learn remote protocol addresses [Y]?
Is multicast required for this circuit [Y]?
Are call-ins allowed for this circuit [Y]?

Circuit name

Especifica el nombre de circuito para el SVC. Este nombre se utilizará para asociar la llamada con un protocolo y una definición de BRS y se utilizará para identificar una conexión en lugar de un número de circuito.

Valores válidos: Una serie ASCII de 1 a 32 caracteres

Valor por omisión: El nombre es necesario y debe ser exclusivo para esta interfaz

Remote party number

Especifica la dirección Frame Relay del destino remoto.

Valores válidos: Una serie de 1 a 20 caracteres de dígitos decimales

Valor por omisión: Ninguno

Remote party numbering plan

Especifica el formato de un número de parte remota. La planificación de la numeración debe coincidir con la utilizada por la red FR.

Valores válidos: E.164 (RDSI) o X.121 (Data)

Valor por omisión: E.164

Remote party number type

Especifica el tipo de número de parte Frame Relay de destino. El tipo de número debe coincidir con el utilizado por la red FR.

Valores válidos: International o Unknown

Valor por omisión: International

Remote party subaddress

Especifica la entidad de la parte (por ejemplo, protocolo) del nodo de destino. Si se utiliza la subdirección, se hará coincidir con la subdirección del dispositivo remoto. La subdirección de ambos extremos de la conexión debe ser la misma.

El formato de **remote party subaddress** puede ser:

- NSAP

El número de dígitos entrados debe ser par y estar en el rango de X'0' a X'F'.

- Private

Si la codificación es BCD, puede entrarse un número impar de dígitos en el rango de 0 a 9.

Si la codificación no es BCD, puede entrarse un número par de dígitos en el rango de X'0' a X'F'.

La combinación del número de parte remota y la subdirección de parte remota debe ser exclusiva en esta interfaz y en cualquier subinterfaz asociada. Si son necesarias conexiones paralelas entre dos interfaces de direccionador, debe utilizarse la subdirección para identificar exclusivamente cada definición de conexión virtual conmutada.

Configuración de interfaces Frame Relay (Talk 6)

Valores válidos: Serie de 1 a 40 caracteres hexadecimales

Valor por omisión: Ninguno

Requested outgoing throughput (CIR)

Especifica la CIR de salida pedida. La red proporcionará este ancho de banda, si está disponible.

Valores válidos: La CIR puede ser 0 o un valor en el rango de 300 bps a 2 048 000 bps.

Nota: Los valores válidos para una interfaz FR de un adaptador HSSI son: 0 ó de 300 a 52 000 000

Valor por omisión: El valor por omisión se determina de acuerdo a los valores por omisión de la CIR a nivel de interfaz

Minimum acceptable outgoing Committed Information Rate (CIR)

Especifica la CIR mínima que se aceptará si la red no puede proporcionar la CIR pedida.

Valores válidos: La CIR puede ser 0 o un valor en el rango de 300 bps a 2 048 000 bps con el máximo de **requested outgoing throughput (CIR)**.

Nota: Los valores válidos para una interfaz FR de un adaptador HSSI son: 0 ó de 300 a 52 000 000

Valor por omisión: El valor por omisión se determina de acuerdo a los valores por omisión de la CIR a nivel de interfaz

Requested incoming CIR

Especifica la CIR de entrada pedida.

Valores válidos: La CIR puede ser 0 o un valor en el rango de 300 bps a 2 048 000 bps.

Nota: Los valores válidos para una interfaz FR de un adaptador HSSI son: 0 ó de 300 a 52 000 000

Valor por omisión: El valor de **requested outgoing CIR**

Minimum acceptable incoming Committed Information Rate (CIR)

Especifica la CIR mínima que se aceptará si la red no puede proporcionar la CIR pedida.

Valores válidos: La CIR puede ser 0 o un valor en el rango de 300 bps a 2 048 000 bps con el máximo de **requested incoming CIR**.

Nota: Los valores válidos para una interfaz FR de un adaptador HSSI son: 0 ó de 300 a 52 000 000

Valor por omisión: Igual a **minimum acceptable outgoing CIR**

Requested outgoing committed burst size (Bc)

Especifica el tamaño de ráfaga confirmado de salida pedido.

Valores válidos: La CIR puede ser 0 o un valor en el rango de 300 bps a 2 048 000 bps.

Configuración de interfaces Frame Relay (Talk 6)

Nota: Los valores válidos para una interfaz FR de un adaptador HSSI son: 0 ó de 300 a 52 000 000

Valor por omisión: El valor determinado de acuerdo a los valores por omisión de la CIR a nivel de interfaz

Requested incoming committed burst size (Bc)

Especifica el tamaño de ráfaga confirmado de entrada pedido.

Valores válidos: La CIR puede ser 0 o un valor en el rango de 300 bps a 2 048 000 bps.

Nota: Los valores válidos para una interfaz FR de un adaptador HSSI son: 0 ó de 300 a 52 000 000

Valor por omisión: El valor igual a **requested outgoing Bc**

Outgoing excess burst size (Be)

Especifica el tamaño de ráfaga de salida pedido.

Valores válidos: La CIR puede ser 0 o un valor en el rango de 300 bps a 2 048 000 bps.

Nota: Los valores válidos para una interfaz FR de un adaptador HSSI son: 0 ó de 300 a 52 000 000

Valor por omisión: El valor determinado de acuerdo a los valores por omisión de la CIR a nivel de interfaz

Requested incoming excess burst size (Be)

Especifica el tamaño de exceso de ráfaga de entrada pedido.

Valores válidos: La CIR puede ser 0 o un valor en el rango de 300 bps a 2 048 000 bps.

Nota: Los valores válidos para una interfaz FR de un adaptador HSSI son: 0 ó de 300 a 52 000 000

Valor por omisión: Igual a **requested outgoing excess burst size (Be)**

Idle timer

Especifica el período de tiempo que un SVC permanecerá activo en ausencia de tráfico. La especificación de 0 designa este SVC como un circuito fijo que se establecerá la primera vez que lleguen datos para el mismo y no se desconectará aunque no fluya tráfico a través suyo.

Valores válidos: De 0 a 65535 segundos

Valor por omisión: 60

Establish circuit to learn remote protocol addresses

Especifica si este SVC debe establecerse cuando se active la interfaz para reconocer las direcciones de protocolo del nodo adyacente. Esta opción puede utilizarse en lugar de los nombres de protocolo de destino configurados estáticamente y las direcciones para los protocolos que soportan el descubrimiento dinámico de direcciones como, por ejemplo, IP IPX, Appletalk2 y DECnet IV para forzar que el direccionador conozca las direcciones de protocolo asociadas al dispositivo remoto mediante InARP

Configuración de interfaces Frame Relay (Talk 6)

directo. La utilización de esta opción puede ayudar a reducir las difusiones ARP. Se utilizará el temporizador de desocupado para desconectar el SVC una vez se hayan conocido las direcciones de protocolo.

Valores válidos: yes o no

Valor por omisión: yes

Is multicast required for this circuit

Especifica si este SVC debe utilizarse o no para transmitir paquetes de multidifusión en esta interfaz aunque signifique activar el SVC sólo para ello. Puede utilizar rutas estáticas para no tener que pedir la multidifusión en los SVC, para que éstos no se establezcan sólo para intercambiar información de direccionamiento.

Valores válidos: yes o no

Valor por omisión: Toma el valor por omisión de acuerdo al valor de la emulación de multidifusión a nivel de interfaz

Are call-ins allowed

Especifica si una llamada de entrada desde un DTE remoto debe aceptarse o no. Puede utilizarse la especificación de no para bloquear llamadas de entrada de usuarios específicos y ayudar a eliminar condiciones de actualización de llamadas de entrada/salida.

Valores válidos: yes o no

Valor por omisión: yes

Compression capable

Especifica si está soportada la compresión de Frame Relay.

Valores válidos: yes o no

Valor por omisión: yes, si la compresión está habilitada para la interfaz. De lo contrario, no.

Encryption capable

Le permite especificar si el circuito cifrará o no los paquetes de datos. Esta pregunta sólo aparece si el cifrado está habilitado en la interfaz. Las solicitudes de la clave de cifrado y algoritmo sólo aparecerán si activa el cifrado en el SVC.

Specifying the Encryption Key: Debe especificar el valor de clave de cifrado en caracteres hexadecimales.

Valores válidos: 16 para CDMF, 48 para 3DES

Nota: El soporte de cifrado es opcional y debe añadirse a la carga de software utilizando el mandato **load add**. Consulte la sección "Load" en la página 101.

Change

Utilice el mandato **change permanent-virtual-circuit** para cambiar cualquier PCV anterior que se haya añadido con el mandato **add permanent-virtual-circuit**. Si utiliza la fragmentación de tipo de extremo a extremo, utilice el mandato **change permanent-virtual-circuit** para designar los PVC a través de los cuales se llevará a cabo la fragmentación de extremo a extremo.

Configuración de interfaces Frame Relay (Talk 6)

Sintaxis:

```
change                frame-handler-pvc . . .  
                        permanent-virtual-circuit . . .  
                        switched-virtual-circuit . . .
```

Ejemplo:

```
change permanent-virtual-circuit  
Circuit Number [16]?  
Committed Information Rate in bps [64000]?  
Committed Burst Size (Bc) in bits [64000]?  
Excess Burst Size (Be) in bits [0]?  
Assign Circuit Name: []?  
Is the circuit required for interface operation [N]?  
Does the circuit belong to a required PVC group [N]?  
Do you want to have data compression performed [Y]?  
Do you want end-to-end fragmentation performed on this circuit [Y]?  
Fragment size (50 to 8190) [256]?  
Fragmented packet reassembly timer (3 to 10 seconds) [3]?  
Do you want to have data encryption performed [N]?  
Enable circuit for voice forwarding [N]?
```

frame-handler-pvc

Consulte el mandato **add frame-handler-pvc** en la página 562 para ver la descripción de los parámetros.

permanent virtual circuit

Consulte el mandato **add permanent-virtual-circuit** en la página 563 para ver una descripción de los parámetros, excepto los parámetros de fragmentación. Estos se describen en el mandato **enable fragmentation**.

switched-virtual-circuit

```
FR 4 Config>change switched-virtual-circuit  
Circuit name []? svc01  
Remote party number []? 12345  
Remote party number numbering plan (E.164 or X.121) [E.164]?  
Remote party number type (Unknown or International) [International]?  
Remote party subaddress in hexadecimal []? 01  
Remote party subaddress format (private or NSAP) [private]1?  
Requested outgoing Committed Information Rate (CIR) in bps [64000]?  
Minimum acceptable outgoing Committed Information Rate (CIR) in bps [64000]?  
Requested incoming Committed Information Rate (CIR) in bps [64000]?  
Minimum acceptable incoming Committed Information Rate (CIR) in bps [64000]?  
Requested outgoing Committed Burst size (Bc) in bits [64000]?  
Requested incoming Committed Burst size (Bc) in bits [64000]?  
Requested outgoing Excess Burst size (Be) in bits [0]?  
Requested incoming Excess Burst size (Be) in bits [0]?  
Idle timer in seconds [60]?  
Establish circuit to learn remote protocol addresses [Y]?  
Is multicast required for this circuit [Y]?  
Are call-ins allowed for this circuit [Y]?
```

Consulte la página 567 para ver una descripción de los parámetros.

Disable

Utilice el mandato **disable** para inhabilitar las características habilitadas previamente utilizando el mandato **enable**.

Sintaxis:

```
disable                cir-monitor  
                        cllm  
                        compression
```

Configuración de interfaces Frame Relay (Talk 6)

congestion-monitor
dn-length-field
encryption
fragmentation
lmi
lower-dtr
multicast-emulation
no-pvc
notify-fecn-source
orphan-circuits
point-to-point
protocol-broadcast
switched-virtual-circuits
throttle-transmit-on-fecn

Nota: Los parámetros de la lista siguiente pueden habilitarse e inhabilitarse en una subinterfaz FR:

- dn-length-field
- multicast-emulation
- no-pvc
- point-to-point
- protocol-broadcast

Estos parámetros pueden tener valores diferentes en una subinterfaz FR que en la interfaz base FR.

El resto de los parámetros sólo se pueden inhabilitar y habilitar en la interfaz base FR. Los valores de estos parámetros en las subinterfaces FR se determinan por sus valores en la interfaz base FR. Por ejemplo, si se inhabilita el cifrado en la interfaz base FR, también se inhabilita en todas las subinterfaces FR que están asociadas a esa interfaz base.

cir-monitor

La inhabilitación de esta característica permite que la velocidad de información del circuito exceda la velocidad máxima de información que se calcula utilizando los parámetros configurados con los mandatos **add permanent-virtual-circuit** o **add switched-virtual-circuit**. El valor por omisión para esta característica es disabled. Consulte la sección “Congestión de circuitos” en la página 546 para obtener más información.

cllm Inhabilita la *moderación de la velocidad* que efectúa el dispositivo como respuesta a un mensaje CLLM. El valor por omisión es inhabilitada. Consulte la sección “Congestión de circuitos” en la página 546 para ver los detalles.

compression

Inhabilita la compresión en la interfaz. No se efectuará compresión para ningún VC. Las subinterfaces FR asociadas a la interfaz base FR tendrán el mismo valor para la compresión que la interfaz base.

congestion-monitor

Inhabilita la característica de supervisión de la congestión. La inhabilitación

Configuración de interfaces Frame Relay (Talk 6)

de esta característica impide que la velocidad de información de un circuito varíe, como respuesta a una congestión, entre la velocidad mínima de información y la velocidad de línea. Consulte la sección “Congestión de circuitos” en la página 546 para obtener más información. El valor por omisión para esta característica es `enabled`.

dn-length-field

Impide la interoperación con implementaciones de DECnet Phase IV a través de Frame Relay que necesiten que un campo de longitud preceda a los paquetes DECnet en las tramas Frame Relay, pero permite la interoperación con el software DECnet Phase IV Frame Relay que no utiliza un campo de longitud antes del paquete DECnet. La inhabilitación de `dn-length-field` hace que Frame Relay no inserte un campo de longitud en las tramas transmitidas que contienen paquetes DECnet y que no intente eliminar el campo de longitud de las tramas recibidas que contienen paquetes DECnet.

Nota: Esta opción sólo se presenta como una opción de configuración cuando el software del direccionador contiene el protocolo DECnet Phase IV. Esta opción puede establecerse en una subinterfaz FR y puede diferir del valor de la interfaz base FR.

encryption

Inhabilita el cifrado en la interfaz. Aunque los PVC de esta interfaz tengan la posibilidad de cifrado, éste no se realizará. No se puede inhabilitar o habilitar el cifrado para las subinterfaces FR. Las subinterfaces FR tendrán el mismo valor para el cifrado que la interfaz base FR.

Nota: El soporte de cifrado es opcional y debe añadirse a la carga de software utilizando el mandato **load add**. Consulte la sección “Load” en la página 101.

fragmentation

Inhabilita globalmente la fragmentación en esta interfaz. Las subinterfaces FR tendrán el mismo valor para la fragmentación que la interfaz base FR.

Imi La inhabilitación de este parámetro permite un funcionamiento normal o la prueba de Frame Relay de extremo a extremo en ausencia de una red real o interfaz de gestión. Con la prueba de Frame Relay de extremo a extremo, es necesario añadir PVC iguales (el mismo número de PVC como, por ejemplo, 16 y 16) en ambos extremos del enlace. Las subinterfaces Frame Relay asociadas tendrán el mismo valor para este parámetro que la interfaz base Frame Relay.

lower-dtr

Este parámetro determina la forma en que se maneja la señal terminal de datos preparado (DTR) para las interfaces de línea serie alquilada del direccionador. No está soportado en interfaces de circuitos de marcación Frame Relay. Consulte el mandato **enable lower-dtr** para ver una descripción más completa del parámetro `lower-dtr`.

Se da soporte a los tipos de cable siguientes:

- EIA 232 (RS-232)
- V.35
- V.36

El valor por omisión es **disable lower-dtr**.

multicast-emulation

Configuración de interfaces Frame Relay (Talk 6)

Inhabilita la emulación de multidifusión en cada VC activo. El valor por omisión para esta característica es *enabled*. Si inhabilita esta característica, es necesario que añada correlaciones de direcciones estáticas de protocolo. Esta opción puede establecerse en una subinterfaz FR y puede diferir del valor de la interfaz base FR.

Algunos protocolos como, por ejemplo, IPX RIP, no funcionarán en la interfaz Frame Relay si está inhabilitada la emulación de multidifusión. La característica de difusión de protocolos necesita también la emulación de multidifusión para funcionar correctamente. Para obtener más información, consulte la sección “Emulación de multidifusión y difusión de protocolo” en la página 541.

no-pvc

Controla si la interfaz se considera activa o inactiva. Si no-pvc está inhabilitado, la presencia de PVC activos en la interfaz no afecta a si la interfaz Frame Relay se considera activa o inactiva. Esta opción puede establecerse en una subinterfaz FR y puede diferir del valor de la interfaz base FR.

notify-fecn-source

Inhabilita el establecimiento de un bit BECN en el primer paquete destinado a un dispositivo desde el cual el direccionador ha recibido un paquete con el bit FECN establecido. Consulte la sección “Congestión de circuitos” en la página 546 para obtener más información.

orphan-circuits

Prohíbe la utilización de todos los circuitos huérfanos PVC no configurados en la interfaz. El valor por omisión para los circuitos huérfanos es habilitado. La inhabilitación de circuitos huérfanos añade una medida de seguridad a la red, impidiendo la entrada no autorizada de un circuito no configurado. Sin embargo, si inhabilita los circuitos huérfanos, es necesario que añada los PVC que se utilizarán en la interfaz.

point-to-point

Inhabilita el punto a punto en la interfaz. Punto a punto indica que la interfaz es de punto a punto desde la perspectiva de IP. Esta opción puede establecerse en una subinterfaz FR y puede diferir del valor de la interfaz base FR.

protocol-broadcast

Prohíbe que los protocolos como, por ejemplo, IP RIP funcionen en la interfaz Frame Relay. Para obtener más información, consulte la sección “Emulación de multidifusión y difusión de protocolo” en la página 541. El valor por omisión para esta característica es *enabled*. Esta opción puede establecerse en una subinterfaz FR y puede diferir del valor de la interfaz base FR.

switched-virtual-circuits

Prohíbe la utilización de los SVC.

throttle-transmit-on-fecn

Prohíbe que el dispositivo *modere la velocidad* de la transmisión de paquetes como respuesta a un paquete con un bit FECN establecido. El valor por omisión es inhabilitada. Consulte la sección “Congestión de circuitos” en la página 546 para obtener más información.

Configuración de interfaces Frame Relay (Talk 6)

Enable

Utilice el mandato **enable** para habilitar las características de Frame Relay.

Sintaxis:

<u>enable</u>	<u>cir-monitor</u>
	<u>cllm</u>
	<u>compression</u>
	<u>congestion-monitor</u>
	<u>dn-length-field</u>
	<u>encryption</u>
	<u>fragmentation</u>
	<u>lmi</u>
	<u>lower-dtr</u>
	<u>multicast-emulation</u>
	<u>notify-fecn-source</u>
	<u>no-pvc</u>
	<u>orphan-circuits</u>
	<u>point-to-point</u>
	<u>protocol-broadcast</u>
	<u>switched-virtual-circuits</u>
	<u>throttle-transmit-on-fecn</u>

Nota: Los parámetros de la lista siguiente pueden habilitarse e inhabilitarse en una subinterfaz FR:

- dn-length-field
- multicast-emulation
- no-pvc
- point-to-point
- protocol-broadcast

Estos parámetros pueden tener valores diferentes en una subinterfaz FR de los que tienen en la interfaz base FR.

El resto de los parámetros sólo se pueden inhabilitar y habilitar en la interfaz base FR. Los valores de estos parámetros en las subinterfaces FR se determinan por sus valores en la interfaz base FR. Por ejemplo, si se inhabilita el cifrado en la interfaz base FR, también se habilita en todas las subinterfaces FR que están asociadas a esa interfaz base.

cir-monitor

Habilita la característica de supervisión de circuitos. La característica de supervisión de circuitos asegura que la velocidad de información del circuito varíe entre la velocidad mínima de información y la velocidad máxima de información, calculadas utilizando los parámetros configurados con el mandato **add permanent-virtual-circuit** o el mandato **change permanent-virtual-circuit**.

Configuración de interfaces Frame Relay (Talk 6)

Nota: La característica de supervisión de circuitos prevalece sobre la característica de supervisión de la congestión, si existe un conflicto cuando ambas están habilitadas. El valor por omisión para esta característica es disabled.

Para obtener información adicional consulte la sección “Supervisión de CIR” en la página 546.

Nota: Para maximizar la productividad para los circuitos que ejecutan la compresión de datos, no debe habilitar la supervisión de CIR en la misma interfaz en la que ha habilitado la compresión. Debido a que el dispositivo utiliza el tamaño de las tramas no comprimidas para determinar si se sobrepasa la VIR de un PVC y las tramas comprimidas necesitan menos ancho de banda, la CIR de un PVC estará infrautilizada si el dispositivo efectúa una supervisión estricta y no excede la CIR configurada. En su lugar, puede utilizarse la supervisión de la congestión para permitir que el dispositivo reaccione a las indicaciones de congestión enviadas por la red FR para evitar la pérdida de tramas.

cllm Permite que el dispositivo *modere la velocidad* como respuesta a un mensaje CLLM. Póngase en contacto con el proveedor de red FR para ver si está disponible este soporte. Consulte la sección “Congestión de circuitos” en la página 546 para obtener más información.

compression

Habilita la compresión en la interfaz. Todos los VC con capacidad de compresión de la interfaz pueden comprimir paquetes de datos, siempre que haya contextos disponibles y que no se haya excedido el límite del circuito de compresión activo. (Consulte la sección “Configuración y supervisión de compresión de datos” de la publicación *Utilización y configuración de las características* para ver los detalles.) Las subinterfases FR asociadas a la interfaz base FR tendrán el mismo valor para la compresión que la interfaz base.

Nota: Para maximizar la productividad para los circuitos que ejecutan la compresión de datos, no debe habilitar la supervisión de CIR en la misma interfaz en la que ha habilitado la compresión. Debido a que el dispositivo utiliza el tamaño de las tramas no comprimidas para determinar si se sobrepasa la VIR de un VC y las tramas comprimidas necesitan menos ancho de banda, la CIR de un VC estará infrautilizada si el dispositivo efectúa una supervisión estricta y no excede la CIR configurada. En su lugar, puede utilizarse la supervisión de la congestión para permitir que el dispositivo reaccione a las indicaciones de congestión enviadas por la red FR para evitar la pérdida de tramas.

congestion-monitor

Habilita la característica de supervisión de la congestión. Esta característica permite que la velocidad de información de un circuito varíe, como respuesta a la congestión, entre la velocidad mínima de información y la velocidad de la línea.

Nota: La característica de supervisión de circuitos prevalece sobre la característica de supervisión de la congestión, si existe un conflicto cuando ambas están habilitadas. El valor por omisión para esta característica es enabled.

Configuración de interfaces Frame Relay (Talk 6)

Para obtener información adicional sobre la supervisión de la congestión, consulte la sección “Supervisión de la congestión” en la página 547.

dn-length-field

Soporta la interoperación con implementaciones de DECnet Phase IV en Frame Relay que necesitan que un campo de longitud preceda a los paquetes DECnet en tramas Frame Relay. La habilitación de dn-length-field hace que Frame Relay inserte un campo de longitud en las tramas transmitidas que contienen paquetes DECnet y elimine el campo de longitud de las tramas recibidas que contienen paquetes DECnet. Esta opción está inhabilitada por omisión. Por omisión, Frame Relay no insertará ni intentará eliminar el campo de longitud.

Nota: Esta opción sólo se presenta como una opción de configuración cuando el software del direccionador contiene el protocolo DECnet Phase IV. Esta opción puede inhabilitarse y habilitarse para las subinterfaces FR y puede diferir del valor de la red base FR.

encryption

Habilita el cifrado en la interfaz. Todos los VC configurados como habilitados para el cifrado, cifrarán todos los datos transmitidos.

Las subinterfaces FR asociadas con la interfaz base FR tendrá el mismo valor para el cifrado que la interfaz base.

Nota: El soporte de cifrado es opcional y debe añadirse a la carga de software utilizando el mandato **load add**. Consulte la sección “Load” en la página 101.

fragmentation *tipo-fragmentación tamaño-fragmento temporizador-reensamblaje paquete fragmentado*

Habilita la fragmentación en una interfaz. La fragmentación en un circuito hace que las tramas superiores al tamaño de fragmento se dividan en porciones menores y se transmitan como tramas separadas. Si está habilitada la fragmentación de extremo a extremo, las tramas inferiores al tamaño de fragmento no se enviarán con una cabecera de fragmentación y se pueden intercalar entre fragmentos de otras tramas. La fragmentación debe habilitarse para los circuitos que reenvían tramas de voz o que se comunican con otra interfaz que reenvía tramas de voz. Sin embargo, observe que la fragmentación y el intercalado pueden realizarse para cualquier dato de prioridad alta; es decir, el intercalado está soportado para protocolos que no son de voz a través de Frame Relay.

Recuerde que debe configurar el Sistema de reserva de ancho de banda (BRS) cuando habilite la fragmentación para dar prioridad al tráfico de tiempo real como, por ejemplo, la voz. Para obtener información sobre la reserva de ancho de banda en Frame Relay, consulte las secciones “Utilización de reserva de ancho de banda y puesta en cola con prioridad” y “Configuración y supervisión de reserva de ancho de banda” de la publicación *Utilización y configuración de las características*.

Las subinterfaces FR asociadas con la interfaz base FR tendrá el mismo valor para la fragmentación que la interfaz base FR.

tipo-fragmentación

Los valores de este parámetro son:

- User Network Interface (UNI)/ Network-to-Network Interface (NNI)
- De extremo a extremo

Configuración de interfaces Frame Relay (Talk 6)

User Network Interface (UNI)/Network-to-Network Interface (NNI) es el tipo por omisión. UNI es la fragmentación DTE para DCE; NNI es la fragmentación DCE para DCE y extremo a extremo es la fragmentación DCE para DCE a través de los PVC especificados en particular de la interfaz.

Cuando está habilitada la fragmentación UNI/NNI, se produce la fragmentación para todos los circuitos de la interfaz, incluyendo los PVC de gestión, es decir, DLCI 0. Cuando se configura la fragmentación en un PVC, el tipo de fragmentación para ese circuito siempre es de extremo a extremo. Debe habilitar la fragmentación de extremo a extremo para ambos extremos del PVC cuando se realiza la fragmentación. Sin embargo, no es necesario que el tamaño de fragmento se igual en ambas direcciones.

Si la vía de acceso para el siguiente direccionador pasa a través de un conmutador Frame Relay, debe utilizar el tipo de fragmentación de extremo a extremo. Si utiliza una conexión UNI/NNI del 2216 al siguiente direccionador, asegúrese de que el proveedor de red Frame Relay soporte la fragmentación UNI/NNI.

Valores válidos: UNI/NNI o extremo a extremo

Valor por omisión: UNI/NNI

fragment-size

Visualiza el tamaño de fragmento de cada fragmento en bytes. Para la fragmentación UNI/NNI, este parámetro especifica el tamaño de fragmento utilizado para todos los circuitos de la interfaz. Para la fragmentación de extremo a extremo, este parámetro especifica el tamaño de fragmento por omisión para los PVC de esta interfaz.

Los tamaños de fragmento no se negocian y no es necesario que sean iguales en ambos lados del PVC. Sin embargo, la trama enviada no puede ser mayor que la MTU del extremo receptor del PVC, sin tener en cuenta el tamaño de fragmento. Si la trama excede la MTU del extremo receptor, cuando llega el fragmento que sobrecarga el receptor, éste realizará una de las acciones siguientes:

1. enviar un mensaje de error indicando que no puede almacenar temporalmente el fragmento
2. eliminar este fragmento
3. visualizar el mensaje *Out of sequence fragments*
4. al final eliminar todos los fragmentos de esa trama

Consejos para seleccionar el tamaño de fragmento:

- Cuando especifique el tamaño de fragmento, asegúrese de que el tamaño de fragmento sea el adecuado para la capacidad del enlace. El tamaño de fragmento elegido debe basarse en la velocidad de acceso y en la cantidad de retardo que se tolera para los datos en tiempo real que comparten el enlace.
- Además, se asignan almacenamientos intermedios del direccionador para cada fragmento. Si el tamaño de trama es grande y el tamaño de fragmento muy pequeño, el direccionador

Configuración de interfaces Frame Relay (Talk 6)

puede asignar tantos almacenamientos intermedios a los fragmentos que se degrade el rendimiento del direccionador.

Valores válidos: De 50 a 8190 bytes

Valor por omisión: 256 bytes

fragmented-packet-reassembly-timer

Visualiza el período de tiempo en segundos que el receptor de los fragmentos espera a que llegue el siguiente fragmento de la secuencia. Si este temporizador caduca antes de que llegue el siguiente fragmento, se eliminan todos los fragmentos recibidos para esta trama.

Valores válidos: De 3 a 10 segundos

Valor por omisión: 3 segundos

Imi Habilita la actividad de la gestión.

Después de emitir el mandato **enable Imi**, utilice el mandato **set Imi-type** para seleccionar la modalidad de gestión para la interfaz Frame Relay. Consulte la sección “Habilitación de la gestión de PVC en Frame Relay” en la página 559. El sistema toma por omisión la gestión ANSI T1.617 Anexo D.

Utilice el mandato **enable Imi** para reanudar la gestión LMI si previamente ha inhabilitado la gestión Frame Relay.

LMI sólo proporciona información acerca de los PVC de una interfaz, no es necesario que se habilite si sólo se utilizan SVC a menos que lo necesite la red. Q.922 determina la posibilidad de utilizar todos los SVC en una interfaz y es un indicador del estado de la interfaz en sí. Cuando hay PVC y SVC en una interfaz, puede que LMI y Q.922 estén activos a la vez.

LMI es una función que sólo puede configurarse en la interfaz base FR, no en las subinterfases FR.

lower-dtr

Este parámetro determina cómo se maneja la señal de terminal de datos preparado (DTR) para las interfaces de línea serie alquiladas que están inhabilitadas. No está soportado en interfaces de circuitos de marcación Frame Relay. Si este parámetro se establece en “inhabilitado” (valor por omisión), la señal DTR permanecerá activada cuando se inhabilite la interfaz.

Cuando se habilita lower-dtr, DTR se desactivará cuando se inhabilite la interfaz. Este comportamiento puede ser aconsejable en situaciones en las que se ha configurado la interfaz como un enlace alternativo para el Redireccionamiento de WAN y la interfaz está conectada a un módem de marcación de salida que mantiene su conexión de marcación basándose en el estado de la señal DTR.

Si se habilita esta característica y la interfaz está inhabilitada, la señal DTR se desactiva y el módem mantiene desactivada la conexión de marcación. Cuando la interfaz está habilitada, debido a un escenario de seguridad de Redireccionamiento de WAN, se emite el DTR y el módem marca un número almacenado para el sitio de seguridad. Cuando se restaura la interfaz primaria, se inhabilita la interfaz alternativa, el DTR se desactiva y el módem deja en suspenso la conexión de marcación.

Se da soporte a los tipos de cable siguientes:

Configuración de interfaces Frame Relay (Talk 6)

EIA 232 (RS-232)

V.35

V.36

El valor por omisión es **disable lower-dtr**.

multicast-emulation

Habilita la emulación de multidifusión. Esto permite transmitir una trama de multidifusión/difusión en cada VC activo. Esta opción puede establecerse en una subinterfaz FR y puede diferir del valor de la interfaz base FR.

Los protocolos como, por ejemplo, ARP, IPX RIP e IP RIP necesitan que la emulación de multidifusión esté habilitada para funcionar correctamente en la interfaz Frame Relay. Para obtener más información, consulte la sección "Emulación de multidifusión y difusión de protocolo" en la página 541. El valor por omisión para este parámetro es habilitado.

no-pvc

Controla si la interfaz se considera activa o inactiva. Cuando esta característica está habilitada, la interfaz Frame Relay se inactiva cuando no hay ningún PVC activo en la interfaz. Si hay un PVC activo como mínimo, la interfaz Frame Relay se activa al producirse un intercambio LMI satisfactorio entre el direccionador y el conmutador FR. Esta opción puede establecerse en una subinterfaz FR y puede diferir del valor de la interfaz base FR.

notify-fecn-source

Permite el establecimiento de un bit BECN en el primer paquete destinado a un dispositivo desde el cual el direccionador ha recibido un paquete con un bit FECN establecido. Utilice este parámetro para ampliar los mecanismos de control de congestión del dispositivo de una red si los conmutadores FR no establecen una BECN pero establecen una FECN. Consulte la sección "Congestión de circuitos" en la página 546 para obtener más información.

orphan-circuits

Habilita la utilización de todos los circuitos huérfanos no configurados. El valor por omisión para esta característica es *enabled*. Consulte la sección "CIR de circuito virtual permanente huérfano" en la página 543 para obtener información acerca de los valores de CIR por omisión.

point-to-point

Habilita el punto a punto en la interfaz. Punto a punto indica que la interfaz es de punto a punto desde la perspectiva de IP. Esta opción puede establecerse en una subinterfaz FR y puede diferir del valor de la interfaz base FR. Sólo puede definirse un PVC o un SVC en una interfaz punto a punto.

protocol-broadcast

Permite que los protocolos como, por ejemplo, IP RIP funcionen correctamente en la interfaz Frame Relay. La característica de emulación de multidifusión debe habilitarse para que la característica de difusión de protocolos funcione correctamente. El valor por omisión para esta característica es *enabled*. Esta opción puede establecerse en una subinterfaz FR y puede diferir del valor de la interfaz base FR.

switched-virtual-circuits

Permite utilizar los SVC y le solicita el número de red de SVC local, la planificación de la numeración, si están permitidas las llamadas de entrada

Configuración de interfaces Frame Relay (Talk 6)

desde SVC huérfanos, el número de reintentos de marcación de salida realizados por todos los SVC de la interfaz y si la modalidad de emulación de red, que se utiliza en configuraciones de direccionador de posterior a posterior (por ejemplo, circuito de marcación), es necesaria.

También puede utilizar el mandato **enable switched-virtual-circuits** para cambiar los parámetros de interfaz SVC configurados si los SVC ya se han habilitado.

Ejemplo:

```
FR 1 Config> enable switched
Local party number []? 4141990
Local party number numbering plan (E.164 or X.121) [E.164]?
Local party number type (Unknown or International) [International]?
Are call-ins allowed on this interface [Y]?
Call-out redial attempts [2]?
Network emulation mode [N]?
```

Local party number

Especifica la dirección Frame Relay de destino.

Valores válidos: Una serie de 1 a 20 caracteres de dígitos decimales

Valor por omisión: Ninguno

Local party numbering plan

Especifica el formato del número de parte. La planificación de la numeración debe coincidir con la utilizada por la red FR.

Valores válidos: E.164 (RDSI) o X.121 (Data)

Valor por omisión: E.164

Local party number type

Especifica el tipo de número de parte Frame Relay de destino. El tipo de número debe coincidir con el utilizado por la red FR.

Valores válidos: International o Unknown

Valor por omisión: International

Call-ins allowed

Especifica si están permitidas las llamadas de SVC no configurados (huérfanos) en esta interfaz.

Call-out redial attempts

Especifica el número de intentos de remarcaciones de llamada externa que se realizarán para cada SVC en caso de un tiempo de espera excedido de llamada externa en esta interfaz.

Valor por omisión: 2

Network emulation mode

Especifica si este SVC está en modalidad de emulación de red. Se utiliza para una configuración de direccionador de posterior a posterior.

throttle-transmit-on-fecn

Permite que el dispositivo *modere la velocidad* de la transmisión de paquetes como respuesta a un paquete con un bit FECN establecido. Utilice este parámetro para minimizar la congestión de la red FR global siempre que se reciba una indicación de congestión. Hace que el dispositivo reaccione a una FECN de la misma manera que reacciona a una BECN.

List

Utilice el mandato **list** para visualizar la gestión configurada actualmente y la información de PVC.

Sintaxis:

```
list                               all
                                     fragmentation-capable-pvcs
                                     frame-handler-pvcs
                                     hdlc
                                     interface
                                     lmi
                                     permanent-virtual-circuits
                                     protocol-addresses
                                     pvc-groups
                                     subinterfaces
                                     switched-virtual-circuits
                                     voice-forwarding-circuits
```

all Visualiza la configuración de Frame Relay. La visualización es una combinación de los mandatos **list hdlc**, **list lmi**, **list switched-virtual-circuits** y **list permanent virtual circuits**.

fragmentation-capable-pvcs

Visualiza todos los PVC que tienen habilitada la fragmentación de extremo a extremo junto con su tamaño de fragmento y los valores del temporizador de reensamblaje.

frame-handler-pvc

Visualiza cada PVC de manejador de tramas junto con el asociado de direccionamiento para la red especificada.

hdlc Visualiza la configuración de Frame Relay High-Level Data Link Control (HDLC).

Ejemplo de una interfaz base FR:

```
list hdlc                               Frame Relay HDLC Configuration

Maximum frame size   = 2048
Encoding             = NRZ
Idle state           = Flag
Clocking              = External
Cable type           = V.35 DTE
Line speed (bps)     = 64000
Transmit delay       = 0
Lower DTR            = Enabled
```

Ejemplo de una subinterfaz FR:

```
list hdlc interface                    Frame Relay Subinterface Configuration

Frame Relay base network number = 1

Emulate multicast    = Yes   Protocol broadcast    = Yes
Point-to-point      = Yes   Interface down if no PVCs = No
```

Configuración de interfaces Frame Relay (Talk 6)

Encoding

El esquema de codificación de transmisión para la interfaz serie. La codificación es NRZ (sin retorno a cero) o NRZI (inversión sin retorno a cero).

Idle El estado de desocupado del enlace de datos: distintivo o marca.

Clocking

El tipo de cronometraje: interno o externo.

Cable type

El tipo de cable de adaptador serie: RS-232, V.35, V.36 o X.21.

Line Speed (bps)

Indica la velocidad física de datos para la interfaz Frame Relay.

Maximum frame size

Indica el tamaño máximo de trama que puede transmitirse o recibirse en la red en un momento determinado.

Transmit delay

Indica el número de bytes de distintivo adicionales enviados entre tramas.

Lower DTR

Indica si el direccionador desactivará la señal DTR cuando ya no sea necesario un enlace alternativo de Redireccionamiento de WAN. La desactivación de la señal DTR hace que el módem termine la conexión de línea alquilada para el enlace alternativo. El DTR desactivado no aparece cuando el tipo de cable es X.21.

Emulate multicast

Indica si la característica de emulación de multidifusión está habilitada en cada PVC activo, yes o no.

Protocol broadcast

Indica si los protocolos como, por ejemplo, IP RIP pueden funcionar en la interfaz Frame Relay, yes o no.

Point-to-point

Indica si la interfaz es de punto a punto desde una perspectiva IP.

Interface down if no PVCs

Indica si el direccionador considera la interfaz no disponible cuando no hay PVC activos.

Notas:

1. Para una interfaz de circuito de marcación FR, sólo se visualiza el tamaño máximo de trama.
2. Para las interfaces FR del adaptador HSSI, el mandato **list hdlc** sólo visualiza un subconjunto de los parámetros HDLC mostrados arriba.

interface

Si se trata de una interfaz base FR, se visualiza la misma información que con el mandato **list lmi**. Si se trata de una subinterfaz FR, se visualiza la misma información que con el mandato **list hdlc interface**.

lmi Visualiza la gestión lógica y la información de configuración relacionada acerca de la interfaz Frame Relay.

Configuración de interfaces Frame Relay (Talk 6)

Nota: Para las subinterfaces FR, este mandato visualiza la misma información que para el mandato **list hdlc**. Las subinterfaces FR no soportan la gestión LMI.

Ejemplo:

```
Frame Relay Configuration

LMI network type      = UNI LMI DLCI              = 0
LMI type              = ANSI LMI Orphans OK       = Yes
CLLM enabled          = No Timer Ty seconds       = 11
SVC network number    = 15
SVC Number type       = International
SVC Numbering plan    = E.164 SVC Call-out redial attempts = 2
SVC Call-ins allowed  = Yes SVC Network emulation mode = No

Protocol broadcast    = Yes Congestion monitoring     = Yes
Emulate multicast     = Yes CIR monitoring           = No
Notify FECN source    = No Throttle transmit on FECN = No
Point-to-point        = No

Data compression      = No
1
Fragmentation Type = END-TO-END
Fragmentation Size = 440 Fragment reassembly timer = 3

Number VCs P1 allowed = 64 Interface down if no PVCs = No
Timer T1 seconds      = 10 Timer T2 seconds         = 15
LMI N1 increments     = 6 LMI N2 error threshold    = 3
LMI N3 error threshold = 4
MIR % of CIR          = 25 IR % Increment           = 12
IR % Decrement        = 25 DECnet length field      = No
Default CIR           = 64000 Default Burst Size    = 64000
Default Excess Burst  = 0
```

¹ Las dos líneas que siguen a este marcador sólo aparecen cuando la fragmentación está activada (yes).

LMI enabled

Indica si están habilitadas las características de gestión en la interfaz Frame Relay. Si LMI no está habilitada, este valor es *no*; si LMI está habilitada, se visualiza el tipo de red LMMI, UNI o NNI.

LMI DLCI

Indica el número del circuito de gestión. Este número refleja el tipo de LMI: 0 para ANSI y ITU-T/CCITT y 1023 para REV1.

LMI Type

Indica el tipo LMI: REV1, ANSI o CCITT.

LMI Orphans OK

Indica si los circuitos no configurados están disponibles para su utilización, yes o no.

CLLM Enabled

Indica si CLLM está habilitado en la interfaz Frame Relay.

Timer Ty seconds

Indica el período de tiempo que debe transcurrir sin que el dispositivo reciba ningún mensaje CLLM ni ninguna BECN antes de que el dispositivo considere que se ha solucionado una condición de congestión y devuelva gradualmente el PVC a su velocidad de transmisión configurada.

SVC network number

Especifica el número de red para los SVC de esta interfaz.

SVC number type

Especifica el tipo de número SVC, unknown o international.

Configuración de interfaces Frame Relay (Talk 6)

SVC numbering plan

Especifica si la planificación de la numeración es E.164 ó X.121.

SVC call-out redial attempts

Especifica el número de intentos de volver a marcar para llamadas externas de esta interfaz.

SVC network emulation mode

Especifica si esta interfaz funciona en modalidad de emulación de red para los SVC.

SVC call-ins allowed

Especifica si están permitidas las llamadas de entrada en esta interfaz.

Protocol Broadcast

Indica si los protocolos como, por ejemplo, IP RIP pueden funcionar en la interfaz Frame Relay, yes o no.

Emulate multicast

Indica si la característica de emulación de multidifusión está habilitada en cada PVC activo, yes o no.

Congestion Monitoring

Indica si la característica de supervisión de la congestión que responde a la congestión de la red está habilitada, yes o no.

CIR monitoring

Indica si la característica de supervisión del circuito que fuerza la velocidad de transmisión está habilitada, yes o no.

Notify FECN Source

Indica si este dispositivo establece un bit BECN en el primer paquete destinado a un dispositivo desde el cual el direccionador ha recibido un paquete con el bit FECN establecido.

Throttle Transmit on FECN

Indica si el dispositivo *moderará la velocidad* de la transmisión de paquetes como respuesta a un paquete con un bit FECN establecido.

Data compression

Indica si esta interfaz tiene la compresión de datos habilitada.

Data encryption

Indica si esta interfaz tiene el cifrado de datos habilitado y el número de circuitos que tienen la posibilidad de cifrado.

Nota: El soporte de cifrado es opcional y debe añadirse a la carga de software utilizando el mandato **load add**. Consulte la sección "Load" en la página 101.

Fragmentation

Indica si está habilitada la fragmentación en esta interfaz.

Fragmentation type

Visualiza el tipo de fragmentación: UNI/NNI (interfaz User-to-Network/interfaz Network-to-Network) o de extremo a extremo, que es la fragmentación por los DTE similares a través de un PVC especificado.

Fragment size

Visualiza el tamaño de fragmento de cada fragmento en bytes.

Configuración de interfaces Frame Relay (Talk 6)

Fragmentation timer value

Visualiza el período de tiempo en segundos que el receptor de los fragmentos espera a que llegue el siguiente fragmento. Si este temporizador caduca antes de que llegue el siguiente fragmento, se eliminan todos los fragmentos recibidos para esta trama.

Orphan compression

Indica si los circuitos huérfanos de esta interfaz tendrán habilitada la compresión de datos.

Nota: La habilitación de la compresión en circuitos huérfanos disminuirá el número de contextos de compresión disponibles para los PVC nativos del dispositivo.

La compresión de huérfanos se aplica a los PVC y los SVC.

Compression circuit limit

Indica el número máximo de circuitos que pueden participar en la compresión de datos.

Number of compression VCs

Indica el número actual de VC que soportan la compresión de datos.

P1 allowed

Indica la suma total de PVC y SVC permitidos para utilizar con esta interfaz, incluyendo la interfaz base FR y cualquier subinterfaz asociada a la interfaz base.

Timer T1 seconds

Indica la frecuencia con la que la interfaz Frame Relay realiza un intercambio de números de secuencia con la entidad LMI de conmutador Frame Relay.

Counter N1 increments

Indica el número de intervalos del temporizador T1 que deben caducar antes de que se realice una consulta completa de estado PVC LMI.

LMI N2 error threshold

Indica el número de errores de sucesos de gestión producidos en la ventana N3 que provocarán un restablecimiento de la interfaz Frame Relay.

LMI N3 error threshold window

Indica el número de sucesos de gestión supervisados utilizados para medir el umbral de errores N2.

MIR % of CIR

IR mínima, expresada como un porcentaje de CIR.

IR % Increment

Porcentaje en que el direccionador incrementa la IR cada vez que recibe una trama sin ninguna BECN hasta que alcanza la IR máxima.

IR % Decrement

Porcentaje en que el direccionador reduce la IR cada vez que recibe una trama que contiene una BECN hasta que llega a la IR mínima.

Configuración de interfaces Frame Relay (Talk 6)

Default CIR

La velocidad de información confirmada, en bps, utilizada como valor por omisión para los VC de esta interfaz.

Default Burst Size

El tamaño de ráfaga confirmado, en bits, utilizado como valor por omisión para los VC de esta interfaz.

Default Excess Burst Size

El tamaño de exceso de ráfaga, en bits, utilizado como valor por omisión para los VC de esta interfaz.

permanent-virtual-circuits

Visualiza todos los PVC configurados en la interfaz Frame Relay.

Ejemplo:

```
FR 1 Config>list permanent virtual circuits
Maximum circuits allowable =      64
Circuits configured this interface =    2
PVCs configured this interface =    1
Total circuits configured =    4
Total PVCs configured =    2
```

Circuit Name	Circuit Number	Options	CIR in bps	Burst Size	Excess Burst
-----	-----	-----	-----	-----	-----
circ16	16	c	64000	64000	0

R = circuit is required
G = circuit is required and belongs to a required PVC group
F = circuit is fragmentation capable
c = circuit is data compression capable
d = circuit is CDMF data encryption capable
t = circuit is triple-DES data encryption capable
V = circuit is voice forwarding enabled
H = frame handler circuit

Maximum circuits allowable

Indica el número de PVC y SVC que pueden existir para esta interfaz, incluyendo la interfaz base FR y todas las subinterfases que están asociadas a la interfaz base FR. Este número incluye cualquier PVC que haya añadido con el mandato **add permanent-virtual-circuit** y cualquier SVC que haya añadido con el mandato **add switched-virtual-circuit** y haya conocido dinámicamente a través de la interfaz de gestión.

Circuits configured this interface

Indica el número de PVC y SVC configurados actualmente para esta interfaz. Esta interfaz es una interfaz base FR o una subinterfaz FR.

PVCs configured this interface

Indica el número de PVC configurados actualmente para esta interfaz, ya sea una interfaz base FR o una subinterfaz FR.

Total circuits configured

Indica el número total de PVC y SVC configurados actualmente que existen para la interfaz base FR y las subinterfases.

Total PVCs configured

Indica el número total de PVC configurados actualmente que existen para la interfaz base FR y las subinterfases.

Circuit Name

Indica la designación ASCII del PVC configurado.

Configuración de interfaces Frame Relay (Talk 6)

Circuit Number

Indica el DLCI de un PVC configurado actualmente.

Options

Consulte la lista de opciones de la parte inferior de la pantalla para ver las definiciones.

Committed Information Rate

Indica la velocidad de información a la que la red acuerda transferir los datos bajo condiciones normales.

Committed Burst Size

La cantidad máxima de datos en bits que la red acuerda entregar durante un intervalo de medición igual a (Tamaño de ráfaga confirmado/CIR) segundos.

Excess Burst Size

La cantidad máxima de datos no confirmados en bits que exceden el tamaño de ráfaga confirmado que la red intenta entregar durante un intervalo de medición igual a (Tamaño de ráfaga confirmado/CIR) segundos.

protocol-addresses

Visualiza todas las direcciones de protocolo configuradas estáticamente de las correlaciones de circuitos en la interfaz Frame Relay.

Ejemplo:

```
list protocol-addresses
      Frame Relay Protocol Address Translations

Protocol Type          Protocol Address          Circuit Number or Name
-----
IP                     125.2.29.4                21
IPX                    000000004503              16
```

Protocol Type

Visualiza el nombre del protocolo que se ejecuta en la interfaz.

Protocol Address

Visualiza la dirección de protocolo del dispositivo en el otro extremo del circuito.

Circuit Number or Name

Visualiza el DLCI del PVC o el nombre del SVC que maneja el protocolo.

pvc-groups

Visualiza todos los grupos de PVC necesarios en la interfaz Frame Relay.

Ejemplo:

```
list pvc-groups
      Required PVC group = group1

      Circuit # 16
```

subinterfaces

Lista información de circuito de todos los circuitos, incluyendo los que están en interfaces base FR y subinterfaces FR. Cuando el circuito está en la red base, este mandato visualiza el número de red de la interfaz en la que está el circuito y la palabra *base* entre paréntesis.

Ejemplo:

```
FR 1 Config>list subinterfaces
Maximum circuits allowable =      64
Circuits configured this interface =      2
Total circuits configured   =      4
```

Configuración de interfaces Frame Relay (Talk 6)

Circuit Name	Circuit Number	Remote Party Number	Interface
circ16	16		1 (base)
circ17	17		4
svc1		998	1 (base)
svc2		998	4

Maximum circuits allowable

Indica el número de circuitos que pueden existir para esta interfaz, ya sea la interfaz base FR o la subinterfaz FR.

Circuits configured this interface

Indica el número de PVC y SVC configurados actualmente para esta interfaz, ya sea una interfaz base FR o una subinterfaz FR.

Total circuits configured

Indica el número total de circuitos configurados actualmente para la interfaz base FR y las subinterfaces.

switched-virtual-circuits

```
FR 0 Config>LIST SWITCHED-VIRTUAL-CIRCUITS
```

```
Maximum circuits allowable = 64
Circuits configured this interface = 2
SVCs configured this interface = 1
Total circuits configured = 5
```

Circuit Name	Options	Idle Timer		Outgoing Value	Incoming Value
SVC1	ILM c	60	CIR:	64000	64000
Remote party number: IE3445667			Min CIR:	64000	64000
Remote subaddress: Pc4456d			Burst:	64000	64000
			Excess:	0	0
svc1	ILM c	60	CIR:	64000	64000
Remote party number: IE3445666			Min CIR:	64000	64000
Remote subaddress: P344566			Burst:	64000	64000
			Excess:	0	0

```
Options: I - call-ins allowed, L - learn protocols, M - Multicast required
         c - compression capable, F - UNI/NNI fragmentation enabled
Address type: I - International, U - Unknown
Numbering plan: E - E.164, X - X.121
Subaddress format: N - NSAP, P - private
```

Maximum circuits allowable

Indica el número de circuitos que pueden existir para esta interfaz, ya sea la interfaz base FR o la subinterfaz FR.

Circuits configured this interface

Indica el número de PVC y SVC configurados actualmente para esta interfaz, ya sea una interfaz base FR o una subinterfaz FR.

SVCs configured this interface

Indica el número de SVC configurados actualmente para esta interfaz, ya sea una interfaz base FR o una subinterfaz FR.

Total circuits configured

Indica el número total de circuitos configurados actualmente para la interfaz base FR y las subinterfaces.

Circuit Name

Indica la designación ASCII del circuito configurado.

Committed Information Rate

Indica la velocidad de información a la que la red acuerda transferir los datos bajo condiciones normales.

Configuración de interfaces Frame Relay (Talk 6)

Committed Burst Size

La cantidad máxima de datos en bits que la red acuerda entregar durante un intervalo de medición igual a (Tamaño de ráfaga confirmado/CIR) segundos.

Excess Burst Size

La cantidad máxima de datos no confirmados en bits que exceden el tamaño de ráfaga confirmado que la red intenta entregar durante un intervalo de medición igual a (Tamaño de ráfaga confirmado/CIR) segundos.

Idle Timer

El período de tiempo que el SVC permanecerá activo en ausencia de tráfico.

Options

Indica las opciones configuradas para el circuito.

Remote party number

Dirección FR del destino remoto. Esta dirección tiene el prefijo del tipo de dirección y la planificación de numeración utilizada.

Remote subaddress

La subdirección de la parte remota asignada a esta conexión. La subdirección tiene el prefijo del formato de subdirección.

voice-forwarding-circuits

```
FR 2 Config>list voice
```

Circuit Name	Circuit Number	Forwarding Network	Forwarding Circuit
-----	-----	-----	-----
circ11	17	0	16

Circuit Name

Indica la designación ASCII del circuito configurado.

Circuit Number

Indica el circuito para este PVC.

Forwarding Network

Indica el número de red a la cual este circuito reenvía tramas de voz.

Forwarding Circuit

Indica el número de circuito al cual este circuito reenvía tramas de voz.

LLC

Utilice el mandato **LLC** para acceder al entorno de configuración LLC. Consulte la sección "Mandatos de configuración LLC" en la página 251 para ver una explicación de cada uno de estos mandatos.

Nota: El mandato **LLC** sólo está soportado si APPN está en la carga de software.

Sintaxis:

llc

Configuración de interfaces Frame Relay (Talk 6)

Remove

Utilice el mandato **remove** para suprimir cualquier PVC, Grupo PVC necesario, pvc de manejador de tramas o dirección de protocolo que se haya añadido previamente utilizando el mandato **add**.

Sintaxis:

```
remove                frame-handler-pvc . . .  
                        permanent-virtual-circuit . . .  
                        protocol-address  
                        pvc-group  
                        switched-virtual-circuit nombre-circuito
```

frame-handler-pvc *númeropvc*

permanent-virtual-circuit *númeropvc*

Suprime cualquier PVC configurado en el rango de 16 a 1007.

Notas:

1. Cuando suprima un PVC que ejecute la compresión, la interfaz reducirá la cuenta de PVC de compresión activos. Si esta acción reduce la cuenta de PVC de compresión por debajo del límite, recibirá un mensaje indicándolo.
2. Cuando suprima un PVC que ejecute el cifrado, la interfaz reducirá la cuenta de PVC de cifrado activos.

Nota: El soporte del cifrado es opcional y debe añadirse a la carga del software utilizando el mandato **load add**. Consulte el mandato **load** del proceso de configuración en el manual *Nways Multiprotocol Access Services Guía del usuario de software*.

El uso del cifrado múltiple (utilizar el cifrado en la Capa de seguridad de IP y en la Capa de enlace de datos de PPP o Frame Relay) en el direccionador está restringido por la legislación de exportación del Gobierno de los Estados Unidos. Sólo está soportado en cargas de software bajo un estricto control de la exportación (cargas de software que dan soporte a RC4 con claves de 128 bits y DES triple).

protocol-address

Suprime cualquier dirección de protocolo configurada (entradas ARP estáticas). Este parámetro le solicita una información diferente dependiendo del tipo de protocolo que esté añadiendo.

Ejemplo:

```
remove protocol-address  
Protocol name or number [IP]?
```

Protocolo IP:

```
IP Address [0.0.0.0]?  
Circuit Name or Number [16]?
```

Protocolo IPX:

```
Host Number (in hex)[]?  
Circuit Name or Number [16]?
```

Configuración de interfaces Frame Relay (Talk 6)

Protocolo AppleTalk Phase 2:

Network Number (1-65279) []?
Node Number (1-253) []?
Circuit Name or Number [16]?

Protocolo DN:

Node address [0.0]?
Circuit Name or Number [16]?

Protocol name or number

Define el nombre o el número de protocolo que está suprimiendo.
Si intenta suprimir un protocolo no soportado, el sistema visualizará el mensaje de error:

Unknown protocol name, try again

Para ver una lista de protocolos soportados, escriba ? en la solicitud Protocol name or number [IP]?

IP Address

Define la dirección internet de 32 bits del sistema principal IP remoto en notación decimal con puntos.

Host Number

Define la dirección de nodo de 48 bits del sistema principal IPX remoto.

Network Number

Define el número de red AppleTalk Phase 2.

Node Number

Define el número de nodo de la interfaz conectada al sistema principal AppleTalk remoto.

Node address

Define la dirección de nodo DECnet del sistema principal DECnet remoto. Configure la dirección de nodo en el formato x,y, donde x es una dirección de área de 6 bits e y es un número de nodo de 10 bits.

Circuit Number

Define el nombre de un PVC o SVC a través del cual se ejecuta el protocolo.

pvc-group *nombregrupo*

Suprime cualquier grupo PVC configurado por nombre. El grupo sólo se elimina si no tiene ningún circuito miembro.

Ejemplo: remove pvc-group PVC group name [IP]?

switched-virtual-circuit

Suprime cualquier SVC configurado por nombre de circuito.

Set

Utilice el mandato **set** para configurar la interfaz para ejecutar el protocolo Frame Relay.

Nota: El mandato **set** de Talk 6 no se puede aplicar a las subinterfaces.

Consideraciones del mandato set

Configuración de interfaces Frame Relay (Talk 6)

Dos parámetros, el parámetro n2 y el parámetro n3, necesitan una explicación más profunda antes de configurarlos. El parámetro n2 establece el umbral de error para los sucesos de gestión y el parámetro n3 establece el número de sucesos que se supervisan en la ventana de sucesos. Si el número de errores de gestión de la ventana de sucesos es igual a n2, se restablece la interfaz Frame Relay. Por ejemplo:

```
set n3-parameter 4
set n2-parameter 3
```

Ahora tiene un tamaño de ventana de 4 ($n3 = 4$) y un umbral de error de 3 ($n2 = 3$). Esto significa que el sistema está supervisando 4 sucesos de gestión y comprobando si alguno de ellos es erróneo. Si el número de sucesos erróneos es igual a 3 (el parámetro n2), se restablece la interfaz Frame Relay y el estado de la red se considera como *red desactivada*.

Para que el estado de la red se considere como *red activada*, el número de sucesos erróneos de la ventana debe ser menor que el n2 anterior a cualquier cambio del estado.

Sintaxis:

```
set
  cable*
  cir-defaults
  clocking*
  crc-type*
  encoding*
  frame-size
  idle . . .*
  ir-adjustment . . .
  line-speed*
  lmi-network-type
  lmi-type
  n1-parameter
  n2-parameter
  n3-parameter
  p1-parameter
  redials
  t1-parameter
  t2-parameter
  transmit-delay . . .*
  ty-parameter
```

* **Nota:** Los mandatos en los que aparece un * al final no están disponibles para las interfaces de circuito de marcación FR.

Configuración de interfaces Frame Relay (Talk 6)

cable *tipo-enlace-interfaz-física tipo-conexión-datos*

Establece el tipo de cable para el enlace físico de la red.

Se utiliza un cable DTE al conectar el direccionador a algún tipo de dispositivo DCE (por ejemplo, un módem o una DSU/CSU). Se utiliza un cable DCE cuando el direccionador actúa como DCE y proporciona el cronometraje para la conexión directa.

Las opciones disponibles son:

Tipo de enlace de interfaz físico	Tipo de conexión de datos
EIA 232 (RS-232)	DTE, DCE
V35	DTE, DCE
V36	DTE, DCE
X21	DTE, DCE
HSSI	DTE, DCE (vea la nota)

Nota: Cuando se utiliza el cable HSSI DCE, el otro dispositivo también debe estar configurado para utilizar un cable HSSI DCE.

cir-defaults

Establece los valores por omisión para los parámetros de congestión del circuito. Los parámetros son:

cir Establece el valor por omisión de *cir* en el valor proporcionado por un proveedor de red Frame Relay.

Valores válidos: 0 o de 300 a 204 800 bps

Valor por omisión: 64 000

Para HSSI, el valor máximo que puede configurarse es 52 000 000 bps.

bc Establece el valor por omisión de *bc* en el valor proporcionado por un proveedor de red Frame Relay.

Valores válidos: Consulte la sección "Tamaño de ráfaga confirmado (Bc)" en la página 544

Valor por omisión: 64 000

Para HSSI, el valor máximo que puede configurarse es 52 000 000 bps.

be Establece el valor por omisión de *be* en el valor proporcionado por un proveedor de red Frame Relay.

Valores válidos: Consulte la sección "Tamaño de exceso de ráfaga (Be)" en la página 544

Valor por omisión: 0

Para HSSI, el valor máximo que puede configurarse es 52 000 000 bps.

Ejemplo:

```
FR 6 config> set cir-default
Default Committed Information Rate (CIR) in bps [64000]? 48000
Default Committed Burst Size (Bc) in bits [64000]? 40000
Default Excess Burst Size (Be) in bits [0]? 52000
```

Configuración de interfaces Frame Relay (Talk 6)

clocking [external o internal]

Para conectar con un módem o DSU, configure el cronometraje externo y seleccione el cable DTE adecuado con el mandato **set cable**. Utilice el mandato **set line-speed** para configurar la velocidad de línea.

Para conectar directamente con otro dispositivo DTE, configure el cronometraje interno, seleccione el cable DCE adecuado con el mandato **set cable** y configure el cronometraje/velocidad de línea con el mandato **set line-speed**.

Valor por omisión: external

Nota: El tipo de cronometraje no se puede configurar cuando Frame Relay está configurado en un adaptador HSSI. El tipo de cronometraje se determina por el tipo de cable. El cronometraje interno se utiliza cuando está configurado el tipo de cable HSSI DCE y el cronometraje externo se utiliza cuando está configurado el tipo de cable HSSI DTE.

crc-type [crc-ccitt-16 o crc-ccitt-32]

El tipo CRC se puede configurar como CRC de 16 bits o CRC de 32 bits. El valor por omisión es **crc-ccitt-16**.

Nota: El tipo CRC sólo puede configurarse para una interfaz FR de un adaptador HSSI.

codificación [NRZ o NRZI]

Establece el esquema de codificación de transmisión HDLC como NRZ (sin retorno a cero) o NRZI (inversión sin retorno a cero). La mayoría de configuraciones utilizan NRZ, que es el valor por omisión.

Nota: La codificación se establece en NRZ para una interfaz FR en un adaptador HSSI y no es configurable.

frame-size *número*

Establece el tamaño máximo de la parte de la capa de red de las tramas transmitidas y recibidas en la interfaz. El tamaño máximo incluye la dirección DLCI de 2 bytes y los datos de usuario mostrados en la figura 39-4. El tamaño que configure debe ser coherente con el tamaño máximo de trama soportado por el conmutador Frame Relay y por los demás DTE FR de la red Frame Relay. Los valores son de 262 a 8190. El valor por omisión es 2048. Ya que el tamaño de trama configurado incluye la dirección DLCI y la cabecera de encapsulación de multiprotocolo FR RFC 1490 y RFC 2427, el tamaño máximo de paquete de protocolo que puede transmitirse es menor que el tamaño de trama configurado y es dependiente de protocolo. La tabla siguiente muestra cuántos bytes se han de restar del tamaño de trama configurado para determinar el tamaño máximo de paquete de protocolo que puede transmitirse y recibirse en la interfaz.

IP	4 bytes
IPX	10 bytes
Appletalk Phase 2	10 bytes
DECnet Phase IV (DNA IV)	12 bytes
Banyan Vines	10 bytes
OSI	10 bytes
Bridging	10 bytes
APPN	58 bytes (ver la nota)

Configuración de interfaces Frame Relay (Talk 6)

Nota: Supone el peor caso de APPN BAN en el que se añaden una cabecera de dirección MAC T/R y una cabecera LLC además de los bytes de cabecera FR.

Si el cifrado de datos FR está habilitado, debe restar hasta 12 bytes adicionales.

Cuando se utilizan los SVC de Frame Relay, el tamaño máximo de campo de información debe ser igual en ambos extremos del circuito virtual. Para determinar el tamaño máximo de campo de información, reste 16 bytes del tamaño de trama si está habilitado el cifrado en el SVC y reste 4 bytes si el cifrado no está habilitado en el SVC.

idle [flag o mark]

Establece el estado de desocupado de transmisión para la trama HDLC. El valor por omisión es **flag**, que proporciona distintivos continuados (7E hex) entre tramas. La opción de marca pone la línea en estado de marca (OFF, 1) entre tramas.

Nota: Idle se establece en **flag** para una interfaz FR de un adaptador HSSI y no es configurable.

ir-adjustment %-incremento %-decremento IR-mínima

Establece la velocidad mínima de información (IR) y los porcentajes para incrementar o decrementar la IR en respuesta de la congestión de la red.

La IR mínima, expresada como porcentaje de CIR, es el límite inferior de la velocidad de información. El porcentaje mínimo es 1 y el porcentaje máximo es 100. El valor por omisión es 25.

Cuando desaparece la congestión de la red, la velocidad de información aumenta gradualmente en el porcentaje de incremento de ajuste de IR hasta que se alcanza la velocidad máxima de información. El porcentaje mínimo es 1 y el porcentaje máximo es 100. El valor por omisión es 12.

Cuando se produce una congestión de la red, la velocidad de información se reduce en el porcentaje de decremento del ajuste de IR cada vez que se recibe una trama que contiene una BECN hasta que se alcanza la velocidad mínima de información. El porcentaje mínimo es 1 y el porcentaje máximo es 100. El valor por omisión es 25.

Ejemplo:

```
set ir-adjustment
IR adjustment % increment [12]?
  IR adjustment % decrement [25]?
    Minimum IR as % of CIR [25]?
```

line-speed velocidad

Para el cronometraje interno, utilice este mandato para especificar la velocidad de las líneas de reloj de transmisión y recepción.

Para el cronometraje externo, este mandato no afecta al funcionamiento de la WAN/línea serie pero establece la velocidad que algunos protocolos, como IPX, utilizan para determinar los parámetros de coste de direccionamiento. Debe establecer la velocidad de manera que coincida con la velocidad real de la línea. Si no está configurada la velocidad, los protocolos suponen una velocidad de 1 000 000 bps.

Valores válidos:

Cronometraje interno: Consulte la Tabla 72 en la página 598 Cronometraje externo: Co

Configuración de interfaces Frame Relay (Talk 6)

Tabla 72. Velocidades de línea cuando se utiliza el cronometraje interno para interfaces 2216

Tipo de adaptador	Rango de velocidades
EIA 232 de 8 puertos	De 9600 a 64 000 bps
V.35/V.36 de 6 puertos	De 9600 a 460 800 bps, 1 544 000 bps ó 2 048 000 bps
X.21 de 8 puertos	De 9600 a 460 800 bps, 1 544 000 bps ó 2 048 000 bps
HSSI de 1 puerto	22 368 000 bps ó 44 736 000 bps

Tabla 73. Velocidades de línea cuando se utiliza el cronometraje externo para interfaces 2216

Tipo de adaptador	Rango de velocidades
EIA 232 de 8 puertos	De 2400 a 64 000 bps
V.35/V.36 de 6 puertos	De 2400 a 2 048 000 bps
X.21 de 8 puertos	De 2400 a 2 048 000 bps
HSSI de 1 puerto	De 1 544 000 bps a 52 000 000 bps

lmi-network-type

Especifica cómo funciona la interfaz con respecto a LMI.

Nota: El tipo de red LMI debe ser compatible con el nodo FR adyacente. Por ejemplo, si el nodo adyacente está configurado como UNI, esta interfaz FR debe configurarse con un tipo NUI de red LMI y, cuando se utilice el soporte NNI, tanto esta interfaz como la interfaz del nodo FR adyacente deben utilizar un tipo de red NNI.

Valores válidos:

- UNI - interfaz de usuario a red
- NUI - interfaz de red a usuario
- NNI - interfaz de red a red

Valor por omisión: UNI

lmi-type [rev1 o ansi o ccitt]

Establece el tipo de gestión para la interfaz. Consulte la sección "Habilitación de la gestión de PVC en Frame Relay" en la página 559 para obtener detalles sobre la gestión de Frame Relay. El valor por omisión es el tipo **ansi** habilitado.

Tabla 74. Opciones de gestión de Frame Relay

Mandato	Tipo de gestión	Descripción
set	lmi-type rev1	Se ajusta a LMI Revisión 1, (Stratacom's Frame Relay Interface Specification)
set	lmi-type ansi	Se ajusta a ANSI T1.617 RDSI-DSS1-Signalling Specification for Frame Relay Bearer Service (conocido como Anexo D)
set	lmi-type ccitt	Se ajusta al Anexo A de ITU-T/CCITT Recommendation Q.933 - DSS1 Signalling Specification for Frame Mode Basic Call Control.

n1-parameter número

Configura el número de intervalos del temporizador T1 que deben caducar

Configuración de interfaces Frame Relay (Talk 6)

antes de que se realice una consulta completa de estado de PVC. *Número* es el intervalo en el rango de 1 a 255. El valor por omisión es 6.

n2-parameter *númeromáx*

Configura el número de errores que pueden producirse en la ventana de sucesos de gestión supervisada por el parámetro n3 antes de que se restablezca la interfaz Frame Relay. *númeromáx* es un número en el rango de 1 a 10. El valor por omisión es 3. Este parámetro debe ser menor o igual al parámetro n3 o recibirá un mensaje de error.

n3-parameter *númeromáx*

Configura el número de sucesos de gestión supervisados para medir el parámetro n2. *númeromáx* es un número en el rango de 1 a 10. El valor por omisión es 4.

p1-parameter *númeromáx*

Configura el número máximo de PVC soportados por la interfaz Frame Relay. Esto incluye los PVC activos, inactivos, eliminados y congestionados. *númeromáx* es un número en el rango de 0 a 992. El valor por omisión es 64. 0 (cero) implica que la interfaz no da soporte a los PVC.

t1-parameter *tiempo*

Configura el intervalo (en segundos) entre intercambios de números de secuencia con la gestión de Frame Relay. El temporizador T2 de la gestión es el intervalo permitido para que una estación final pida un intercambio de números de secuencia con el gestor. El intervalo T1 debe ser menor que el intervalo T2 de la red. *Tiempo* es un número en el rango de 5 a 30. El valor por omisión es 10.

t2-parameter *tiempo*

Especifica el período de tiempo que FR espera para recibir una consulta de estado de LMI antes de decidir que se ha producido un error, si esta interfaz está configurada con un tipo de red LMI de NUI o NNI. El intervalo t2 debe ser menor que el temporizador t1 del nodo FR adyacente. El valor es un número en el rango de 5 a 30 y el valor por omisión es 15 segundos.

transmit-delay *número*

Permite la inserción de un retardo entre los paquetes transmitidos. El propósito de este mandato es moderar la velocidad de la línea serie para que sea compatible con los dispositivos serie más antiguos y lentos del otro extremo. También puede evitar la pérdida de paquetes hello de línea serie entre líneas. *número* está entre 0 y 15 distintivos adicionales. El valor por omisión es cero (0). Si se establece este parámetro se proporcionan de 0 a 15 distintivos adicionales entre transmisiones de tramas. La Tabla 75 lista las unidades y los valores del rango para las interfaces serie.

Nota: Si configura un retardo de transmisión que no es cero para una interfaz FR de un adaptador EIA-232E de 8 puertos, un adaptador V.35/V.36 de 6 puertos o un adaptador X.21 de 8 puertos, debe configurar una velocidad de línea utilizando el mandato **set line-speed**.

Tabla 75. Unidades de retardo de transmisión y rango para la interfaz serie 2216

Unidad	Mínimo	Máximo
Distintivos adicionales	0	15

ty-parameter *tiempo*

Configura el intervalo después del cual el dispositivo considera que ha

Configuración de interfaces Frame Relay (Talk 6)

desaparecido una condición de congestión existente indicada por la recepción de un mensaje CLLM. Si el dispositivo recibe un mensaje CLLM antes de que caduque el temporizador, el dispositivo restablece este temporizador.

Valores válidos: De 5 a 30 segundos.

Valor por omisión: 11 segundos.

Acceso al indicador de supervisión de Frame Relay

Para acceder a los mandatos operativos de Frame Relay y para supervisar Frame Relay en el direccionador, lleve a cabo los pasos siguientes:

1. En el indicador OPCON (*), escriba **talk 5**.
2. En el indicador GWCON (+), entre el mandato **interface** para ver una lista de las interfaces configuradas en el direccionador.
3. Entre el mandato **network** seguido por el número de red de la interfaz frame relay. Por ejemplo:

```
+ net 2
Frame Relay Monitoring
FR 2 >
```

Mandatos de supervisión Frame Relay

Esta sección resume y explica los mandatos de supervisión Frame Relay. Utilice estos mandatos para reunir información de la base de datos. La Tabla 76 muestra los mandatos.

Tabla 76. Resumen de los mandatos de supervisión Frame Relay

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado "Cómo obtener ayuda" en la página 10.
Clear	Borra la información de estadísticas de la interfaz Frame Relay.
Disable	Inhabilita la supervisión de CIR y la supervisión de la congestión de la interfaz Frame Relay.
Enable	Habilita la supervisión de CIR y la supervisión de la congestión en la interfaz Frame Relay.
List	Visualiza las estadísticas específicas de la capa de enlace de datos y de la gestión de Frame Relay.
LLC	Visualiza el indicador de supervisión LLC.
Notrace	Inhabilita la posibilidad de rastreo de paquetes para circuitos individuales o para toda la interfaz.
Set	Establece la CIR, el Tamaño de ráfaga confirmado y el Tamaño de exceso de ráfaga para un VC de Frame Relay.
Trace	Habilita la posibilidad de rastreo de paquetes para circuitos individuales o para toda la interfaz.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página 11.

Nota: En esta sección, los términos *número de circuito* y *PVC* son equivalentes al término *identificador de circuito de enlace de datos (DLCI)*.

Clear

Utilice el mandato **clear** para poner a cero los contadores de estadísticas de la interfaz Frame Relay.

Supervisión de interfaces Frame Relay

Nota: Las estadísticas también se pueden borrar utilizando el mandato **clear** de OPCON.

Sintaxis:

clear

Disable

Utilice el mandato **disable** para inhabilitar las características de supervisión de CIR y de supervisión de la congestión de Frame Relay.

El mandato **disable** cambia dinámicamente la configuración del direccionador. Estos cambios se perderán cuando se reinicie el direccionador.

Sintaxis:

disable cir-monitor
 cllm
 congestion-monitor
 notify-fecn-source
 throttle-transmit-on-fecn

Enable

Utilice el mandato **enable** para habilitar las características de supervisión de CIR y de supervisión de la congestión de Frame Relay.

El mandato **enable** cambia dinámicamente la configuración del direccionador. Estos cambios se perderán cuando se reinicie el direccionador.

Sintaxis:

enable cir-monitor
 cllm
 congestion-monitor
 notify-fecn-source
 throttle-transmit-on-fecn

List

Utilice el mandato **list** para visualizar las estadísticas específicas para la capa de enlace de datos y la interfaz Frame Relay.

Sintaxis:

list all
 circuit . . .
 frame-handler-pvcs
 interface
 lmi
 permanent-virtual-circuits

Supervisión de interfaces Frame Relay

pvc-groups
queues
subinterfaces
svcs
switched-virtual-circuit
virtual-circuits
voice-forwarding-circuits

all Visualiza las estadísticas del circuito, de la gestión y del VC de la interfaz Frame Relay. La salida visualizada para este mandatos es una combinación de los mandatos **list lmi** y **list permanent-virtual-circuit**.

circuit nombre o número

Visualiza información detallada de las estadísticas y la configuración del circuito virtual para el VC especificado utilizando el nombre de circuito de entrada o DLCI.

Ejemplo:

```
list circuit 347
```

```
Circuit name = Valencia
```

```
Circuit state      = Active  Circuit is orphan = No
Frames transmitted = 0      Bytes transmitted = 0
Frames received   = 0      Bytes received    = 0
Total FECNs      = 0      Total BECNs       = 0
Times congested  = 0      Times Inactive    = 0
CIR in bits/second = 64000 Potential Info Rate = 56000
Committed Burst (BC) = 1200 Excess Burst (Be) = 54800
Minimum Info Rate = 16000 Maximum Info Rate = 64000
Required         = Yes    PVC group name    = group1

Compression capable = Yes   Operational      = Yes
R-Rs received      = 0     R-Rs transmitted = 0
R-As received      = 0     R-As transmitted = 0
R-R mode discards  = 0     Enlarged frames  = 0
Decompress discards = 0     Compression errors = 0
Compression ratio  = 1.72 to 1 Decompression ratio = 1.10 to 1

Fragmentation type = END-T0-END
Fragmentation Size = 0     Reassembly timer  = 0
Fragments xmitted  = 0     Fragments received = 0
Voice Frames xmitted = 0   Voice Frames rcv'd = 0

Encryption capable = Yes   Operational      = Yes
Encryption errors  = 0     Decryption errors  = 0
Rcv error discards = 0

Current number of xmit frames queued = 0
Xmit frames dropped due to queue overflow = 0
```

Circuit state

Indica el estado del circuito : inactivo, activo o congestionado. Inactivo indica que el circuito no está disponible para el tráfico porque la interfaz Frame Relay está desactivada o porque la entidad de gestión de Frame Relay no ha notificado al protocolo Frame Relay que el circuito está activo. Activo indica que se están transfiriendo datos. Congestionado indica que se está controlando el flujo de datos.

Circuit is orphan

Indica que el circuito tiene un PVC no configurado reconocido a través de la gestión LMI o una llamada de entrada para un SVC no configurado.

Frames/Bytes transmitted

Indica cuántas tramas y bytes ha transmitido este VC.

Supervisión de interfaces Frame Relay

Frames/Bytes received

Indica cuántas tramas y bytes ha recibido este VC.

Total FECNS

Indica el número de veces que se ha notificado a este VC una congestión de entrada o en sentido directo.

Total BECNS

Indica el número de veces que se ha notificado a este VC una congestión de salida o en sentido inverso.

Times congested

Indica el número de veces que se ha congestionado este VC.

Times inactive

Indica el número de veces que este VC ha estado no operativo.

CIR in bits/sec

Indica la velocidad de información del VC en el rango de 300 bps a 2 048 000 bps. También se soporta el valor 0.

Potential Info Rate

Indica la velocidad máxima actual en bps a la que se transmitirán los datos para el circuito. La velocidad de datos real dependerá de las profundidades de cola y las prioridades asociadas al circuito.

Si este campo tiene el valor de "Velocidad de línea", la velocidad máxima de datos es la velocidad de línea real incluso si no se ha configurado la velocidad de línea o se ha configurado incorrectamente para esta interfaz.

Committed Burst (BC)

Cantidad máxima de datos, en bits, que el direccionador puede transmitir durante el *intervalo de tiempo* (T_c). ($T_c = Bc / CIR$.)

Excess Burst (Be)

Cantidad máxima de datos no confirmados en bits que el direccionador puede transmitir en un VC que exceden el Bc durante el intervalo de tiempo (T_c).

Minimum Info Rate

Velocidad mínima de información. La velocidad mínima de información para un VC a la que reduce el direccionador cuando se le notifica una congestión.

Maximum Info Rate

Velocidad máxima de datos. La velocidad máxima de datos a la que el direccionador transmite para un VC.

Required

Sí o No. Si es sí, el PVC es un PVC necesario.

PVC group name

Si el PVC es un miembro de un grupo de PVC necesario, aparece el nombre; de lo contrario aparece "Unassigned".

Compression capable

Indica si el circuito puede comprimir paquetes de datos.

Operational

Indica si la compresión está activada en el circuito. Cuando es que sí, los datos se comprimen en este enlace.

Supervisión de interfaces Frame Relay

R-Rs received

Indica el número de paquetes de petición de restablecimiento que ha enviado el descompresor similar. Un descompresor similar envía una petición de restablecimiento siempre que el similar detecta que no está sincronizado con su compresor similar. Si este número aumenta rápidamente, es que se están perdiendo o dañando paquetes en este circuito.

R-Rs transmitted

Indica el número de paquetes de petición de restablecimiento que se han enviado desde que se ha iniciado la compresión en el circuito. Si este número aumenta rápidamente, es que se están perdiendo o dañando paquetes en este circuito.

R-As received

Indica el número de reconocimientos de restablecimiento recibidos como respuesta a peticiones de restablecimiento. El compresor también envía este paquete para señalar que ha restablecido el histórico de compresión.

R-As transmitted

Se trata del número de reconocimientos de restablecimiento enviados al similar.

R-R mode discards

Indica el número de tramas de datos comprimidos que se han eliminado mientras se esperaba un R-A después de enviar un R-R.

Enlarged frames

Es una cuenta de las tramas que no se han podido comprimir. Normalmente una trama que no se puede comprimir se envía en su formato no comprimido dentro de un tipo de trama de compresión especial, lo que permite que el compresor y descompresor permanezcan sincronizados.

Decompress discards

Indica el número de tramas comprimidas que se han eliminado debido a errores en la descompresión.

Compression errors

Indica el número de tramas que contenían errores de compresión que se han transmitido en un formato descomprimido.

Compression ratio

Indica la eficacia aproximada del compresor.

Decompression ratio

Indica la eficacia aproximada del descompresor.

Fragmentation type

Indica el tipo de fragmentación. Los valores son UNI/NNI y de extremo a extremo. Consulte el mandato **enable fragmentation** de talk 6 para obtener más información.

Fragmentation size

Indica el tamaño del fragmento. Consulte el mandato **enable fragmentation** de talk 6 para obtener más información.

Nota: Si está configurada la fragmentación de extremo a extremo, el tamaño de fragmento muestra el tamaño configurado de la interfaz, no el tamaño de cada PVC.

Supervisión de interfaces Frame Relay

Reassembly timer

Indica el tiempo establecido en el temporizador de reensamblaje de paquetes fragmentados. Si el fragmento siguiente de la secuencia de un paquete fragmentado no puede llegar antes de que caduque el temporizador, se elimina el fragmento cuando llega y se desactivan todos los fragmentos de esta trama.

Encryption capable

Indica si este circuito tiene habilitado el cifrado.

Nota: El soporte de cifrado es opcional y debe añadirse a la carga de software utilizando el mandato **load add**. Consulte la sección "Load" en la página 101.

Operational

Indica si el cifrado está activo en el circuito. Cuando es que sí, se cifran los datos en este enlace.

Encryption errors

Indica el número de tramas que han tenido errores de cifrado.

Decryption errors

Indica el número de tramas que han tenido errores de descifrado.

Rcv error discards

Indica el número de tramas comprimidas que se han eliminado debido a problemas en la recepción.

Current number of xmit frames queued

Indica el número de tramas que FR ha puesto actualmente en cola para este circuito. Estas tramas esperan que haya espacio disponible en la cola de transmisión del manejador de dispositivo serie para esta interfaz.

Xmit frames dropped due to queue overflow

Indica el número de tramas que no se han podido transmitir para este VC debido a un desbordamiento de la cola de salida.

frame-handler-pvcs

Ejemplo:

Frame Relay Frame Handler Configuration

Circuit Name	Circuit Number	Status (L/R)	Forwarding Net/Circuit	Max Queue (L/R)
Raleigh	16	A/A	2/18	10/10

Sum of outbound queue limits =	10	Input buffers allocated =	24
Total congested frms discard =	0	Total frms currently queued =	0
Total BECNs set =	0	Total FECNs set =	0

Local/Remote circuit states: A - Active I - Inactive R - Removed

Status (local/remote)

Indica el estado de este PVC (local), activo o inactivo y el estado de este circuito asociado (remoto) del PVC FH.

Forwarding Net/Circuit

El número de red y el número de circuito del PVC que reenvía.

Max Queue (local/remote)

La longitud máxima de cola configurada para este circuito (local) y su asociado (remoto).

Supervisión de interfaces Frame Relay

Sum of outbound queue limits

La suma de los límites de cola para todos los PVC FH de esta interfaz. Si este número es mayor que el campo *Input buffers allocated*, se eliminarán las tramas de entrada antes de alcanzar el límite de la cola de salida para todos los circuitos FH. Esto se produce porque los almacenamientos intermedios de entrada para esta interfaz se ponen en cola para salida en el circuito asociado de salida.

Input buffers allocated

Los almacenamientos intermedios de entrada asignados para esta interfaz.

Total congested frames discarded

El número total de tramas eliminadas por este circuito FH debido a la congestión de entrada o de salida.

Total frms currently queued

El número total de tramas de salida que están en cola actualmente para este circuito.

Total BECNs set

El número total de veces que se ha establecido BECN en una trama debido a la congestión.

Total FECNs set

El número total de veces que se ha establecido FECN en una trama debido a la congestión.

interface

Para una interfaz base FR, el mandato **list interface** visualiza la misma información que el mandato **list lmi**. Para la subinterfaz FR, este mandato visualiza la misma información que el mandato **list hdlc** de Talk 6.

lmi

Visualiza las estadísticas relevantes para la gestión lógica en la interfaz Frame Relay. Si entra este mandato para una subinterfaz FR, se visualiza la información para su interfaz base FR.

Ejemplo:

```
list lmi
Management Status:
-----
LMI network type = UNI LMI DLCI = 0
LMI type = ANSI LMI Orphans OK = YES
CLLM enabled = No

SVC local net number = 12345678
SVC Number type = International
SVC Numbering plan = E.164 SVC Call-out retries = 2
SVC Call-ins allowed = Yes SVC Network emulation mode = No

Protocol broadcast = Yes Congestion monitoring = Yes
Emulate multicast = Yes CIR monitoring = No
Notify FECN source = No Throttle transmit on FECN = No
Number VCs P1 allowed = 64 Interface down if no PVCs = No
Line speed (bps) = 1000000 Maximum frame size (bytes) = 2048
Timer T1 seconds = 10 Counter N1 increments = 6
LMI N2 threshold = 3 LMI N3 threshold window = 4
MIR % of CIR = 25 IR % Increment = 12
IR % Decrement = 25 DECnet length field = No
Default CIR = 64000 Default Burst Size = 64000
Default Excess Burst = 0
Current receive sequence = 0
Current transmit sequence = 1
Total status enquiries = 9 Total status responses = 0
Total sequence requests = 0 Total responses = 0

Data compression enabled = No
```

Supervisión de interfaces Frame Relay

Data encryption enabled = No
Fragmentation enabled = No

Virtual Circuit Status:

```
-----  
Total allowed      = 64 Total configured    = 2  
Total active       = 0 Total congested   = 0  
Total PVCs left net = 0 Total PVCs join net = 0
```

Management Status:

LMI enabled

Si la gestión de Frame Relay no está activada, el valor es *no*. Si LMI está activada, esta entrada visualiza UNI, NUI o NNI, dependiendo de la interfaz de red que LMI utilice.

LMI DLCI

Indica el número del circuito de gestión. Este número es 0 (valor por omisión ANSI o ITU-T/CCITT) o 1023 (LMI interina REV1).

LMI type

Indica el tipo de gestión de frame relay que se utiliza, ANSI, ITU-T/CCITT o LMI Revisión 1.

LMI orphans OK

Indica si todos los circuitos no configurados reconocidos por la gestión LMI de Frame Relay están disponibles para su utilización (yes o no).

CLLM enabled

Especifica si este circuito moderará la transmisión en la recepción de tramas CLLM.

Timer Ty seconds

Indica el valor del temporizador Ty de CLLM. Este campo sólo se visualiza si CLLM está habilitado.

Last CLLM cause code

Indica el código de causa de la congestión proporcionado en el último mensaje CLLM recibido o **None** si no se ha recibido ningún mensaje CLLM. Este campo sólo se visualiza si CLLM está habilitado.

SVC local net number

Especifica el número de red para los SVC de esta interfaz.

SVC number type

Especifica el tipo de número SVC, unknown o international.

SVC numbering plan

Especifica si la planificación de la numeración es E.164 ó X.121.

SVC call-out retries

Especifica el número de intentos de volver a marcar para llamadas externas de esta interfaz.

SVC network emulation mode

Especifica si esta interfaz funciona en modalidad de emulación de red para los SVC.

SVC call-ins allowed

Especifica si están permitidas las llamadas de entrada en esta interfaz.

Supervisión de interfaces Frame Relay

Protocol broadcast

Indica si los protocolos como, por ejemplo, IP RIP pueden funcionar en la interfaz Frame Relay.

Congestion monitoring

Indica si la característica de supervisión de la congestión que responde a la congestión de la red está habilitada (yes o no).

Emulate multicast

Indica si la característica de emulación de multidifusión está habilitada en cada PVC activo (yes o no).

CIR monitoring

Indica si la característica de supervisión del circuito que fuerza la velocidad de transmisión está habilitada (yes o no).

PVCs P1 allowed

Indica el número de VC permitidos para utilizar con esta interfaz. Este número es el número máximo de VC activos, congestionados, inactivos y eliminados que pueden soportarse en la interfaz.

Interface down if no PVCs

Indica si el direccionador considera la interfaz no disponible cuando no hay PVC activos.

Line speed (bps)

Indica la velocidad de datos configurada de la interfaz Frame Relay.

Timer T1 seconds

Indica la frecuencia con la que la interfaz Frame Relay realiza un intercambio de números de secuencia con la entidad LMI de conmutador Frame Relay.

Counter N1 increments

Indica el número de intervalos del temporizador T1 que deben caducar antes que se realice una consulta completa de estado PVC LMI.

LMI N2 error threshold

Indica el número de errores de sucesos de gestión producidos en la ventana N3 que provocarán un restablecimiento de la interfaz Frame Relay.

LMI N3 error threshold window

Indica el número de sucesos de gestión supervisados utilizados para medir el umbral de errores N2.

MIR % of CIR

IR mínima, expresada como un porcentaje de CIR.

IR % Increment

Porcentaje en que el direccionador incrementa la IR cada vez que recibe una trama sin ninguna BECN hasta que alcanza la IR máxima.

IR % Decrement

Porcentaje en que el direccionador reduce la IR cada vez que recibe una trama que contiene una BECN hasta que llega a la IR mínima.

DECnet length field

Indica si la característica de campo de longitud DECnet está habilitada. Algunas implementaciones de Frame Relay DECnet

Supervisión de interfaces Frame Relay

Phase IV necesitan un campo de longitud entre la cabecera de encapsulación multiprotocolo Frame Relay y el paquete DECnet. Se inserta un campo de longitud si está habilitada la característica de campo de longitud DECnet.

Default CIR

Especifica la CIR por omisión para esta interfaz.

Default Burst Size

Especifica el tamaño de ráfaga por omisión para esta interfaz.

Default Excess CIR

Especifica el tamaño de exceso de ráfaga por omisión para esta interfaz.

Current receive sequence

Indica el número de secuencia de recepción actual que ha recibido la interfaz Frame Relay de la entidad de gestión de Frame Relay.

Current transmit sequence

Indica el número de secuencia de transmisión actual que la interfaz Frame Relay ha enviado a la entidad de gestión Frame Relay.

Total status enquiries

Indica el número total de consultas de estado que la interfaz Frame Relay ha realizado de la entidad de gestión Frame Relay.

Total status responses

Indica el número total de respuestas que la interfaz Frame Relay ha recibido de la entidad de gestión Frame Relay en respuesta a las consultas de estado.

Total sequence requests

Indica el número total de peticiones de número de secuencia que la interfaz Frame Relay ha enviado a la entidad de gestión de Frame Relay.

Total responses

Indica el número total de respuestas de número de secuencia que la interfaz Frame Relay ha recibido de la entidad de gestión de Frame Relay.

Data compression enabled

Indica si la compresión de datos está habilitada en esta interfaz.

Data encryption enabled

Indica si el cifrado de datos está habilitado en esta interfaz.

Nota: El soporte de cifrado es opcional y debe añadirse a la carga de software utilizando el mandato **load add**. Consulte la sección "Load" en la página 101.

Fragmentation enabled

Indica si la fragmentación de paquetes Frame Relay está habilitada en esta interfaz.

Fragmentation type

Sólo se visualiza si la fragmentación de paquetes Frame Relay está habilitada en esta interfaz.

Orphan compression

Indica si los circuitos huérfanos de esta interfaz tendrán habilitada la compresión de datos.

Supervisión de interfaces Frame Relay

Nota: La habilitación de la compresión en circuitos huérfanos reducirá el número de contextos de compresión disponibles para los VC nativos del dispositivo.

La compresión de huérfanos se aplica a los PVC y los SVC.

Compression circuit limit

Especifica el número máximo de VC que pueden comprimir datos en esta interfaz.

Active compression circuits

Especifica el número de VC que comprimen datos actualmente en esta interfaz.

Data encryption enabled

Indica si el cifrado de datos está habilitado en esta interfaz.

Nota: El soporte de cifrado es opcional y debe añadirse a la carga de software utilizando el mandato **load add**. Consulte la sección "Load" en la página 101.

Active encryption circuits

Indica el número de VC que están cifrando datos actualmente.

Virtual Circuit Status:

- *Total allowed*—Indica el número de VC permitidos (incluyendo los huérfanos) cuyo estado es activo, congestionado, eliminado o inactivo para utilizar con esta interfaz.
- *Total configured*—Indica el número total de VC configurados actualmente para esta interfaz.
- *Total active*—Indica el número de VC activos en esta interfaz.
- *Total congested*—Indica el número de VC que moderan su velocidad debido a una congestión en la red.
- *Total PVCs left net*—Indica el número total de PVC que se han eliminado de la red.
- *Total PVCs joined net*—Indica el número total de PVC que se están añadiendo a la red.

permanent-virtual-circuit

Visualiza las estadísticas de capa de enlace generales y la información de configuración para todos los PVC configurados en la interfaz Frame Relay.

Ejemplo:

```
FR 0>LIST PERMANENT-VIRTUAL-CIRCUITS
```

Circuit Number	Circuit Name	Options	Type/State	Frames Transmitted	Frames Received
16	Unassigned	R	P/I	0	0
17	Bigcir	F V	P/I	0	0
18	Unassigned		P/I	0	0

```
Circuit type: 0 - Orphan P - PVC S - SVC
Circuit state: A - Active I - Inactive R - Removed C - Congested
R - Required G - Required and belongs to a PVC group
F - circuit is fragmentation capable
c - Data compression capable but not operational
C - Data compression capable and operational
d - CDMF DES data encryption capable but not operational
D - CDMF DES data encryption capable and operational
t - 3DES data encryption capable but not operational
T - 3DES data encryption capable and operational
V - circuit is voice forwarding enabled
H - Frame Handler circuit
```

Supervisión de interfaces Frame Relay

Circuit#

Indica el DLCI del PVC.

Circuit Name

Nombre del circuito, una serie ASCII.

Orphan Circuit

Indica si el PVC es un circuito no configurado (yes o no).

Type/State

Indica el estado del circuito, A (activo), I (inactivo), P (permanente), C (congestionado) o R (eliminado).

Frames Transmitted

Indica cuántas tramas ha transmitido este PVC.

Frames Received

Indica cuántas tramas ha recibido este PVC.

pvc-groups

Visualiza la información de grupo de PVC necesario para todos los grupos de PVC necesarios. Para cada grupo, consta del nombre de grupo, los circuitos del grupo y el estado (activo, inactivo o eliminado) de cada circuito.

Ejemplo:

```
list pvc-groups
-----
Group name          Circuits in group  Circuit status
-----
group1              16                active
                   44                inactive
                   240               removed
```

queues

Visualiza las cuentas de las tramas transmitidas y recibidas, el número de tramas eliminadas, el número actual de tramas que están en cola y la cuenta superior de colas. La cuenta superior de colas es el número máximo de tramas que se han puesto en cola para este circuito.

Ejemplo:

```
DLCI      Circuit Name          Frames Sent  Frames Rcv'd  Frames Discard  Frames Queued  High Queue
-----
18 Phoenix 11946        12041        2           41           41
```

subinterfaces

Lista información de circuito de todos los circuitos, incluyendo los que están en interfaces base FR y subinterfaces FR. Cuando el circuito está en la red base, este mandato visualiza el número de red de la interfaz en la que está el circuito y la palabra *base* entre paréntesis.

Ejemplo:

```
FR 1>list subinterfaces

Circuit Name          Circuit Number  Circuit Type  Interface Number
-----
svc1                  16             Switched     1 (base)
circ16                16             Permanent   1 (base)
svc2                  17             Switched     4
circ17                17             Permanent   4
```

svcs Visualiza todos los SVC, configurados o huérfanos, de la interfaz sin tener en cuenta el estado.

Ejemplo:

Supervisión de interfaces Frame Relay

FR 1>list svcs

Circuit Name	Remote party number	Circuit State	Call State	DLCI
flotsam	911	R	N	0
jetsam	666	R	N	0

Circuit states: A - Active I - Inactive R - Removed C - Congested
 Call states: N - Null I - Call Initiated O - Outgoing call proceeding
 A - Active D - Disconnect request R - Release request

switched-virtual-circuit

El ejemplo siguiente visualiza información de configuración y operativa para un único SVC por el nombre.

Ejemplo:

FR 1>list switched-virtual-circuit flotsam

Circuit Name	Options	Idle Timer	Outgoing Value	Incoming Value
flotsam	ILMF	60	CIR: 0	0
Call state: Null			Burst: 0	0
Call Initiated by: None		DLCI: 0	Excess: 0	0
Remote party number: IE14				
Remote subaddress: None				

Options: I - call-ins allowed, L - learn protocols, M - multicast required
 F - UNI/NNI fragmentation capable C - compression capable and operational
 c - compression capable, d - CDMF DES data encryption capable but not operational
 D - CDMF DES data encryption capable and operational t - 3DES data encryption capable but not operational T - 3DES data encryption capable and operational
 Address type: I - International, U - Unknown Numbering plan: E - E.164,
 X - X.121 Subaddress format: N - NSAP, P - private

virtual-circuits

Visualiza todos los PVC y todos los SVC activos con información asociada que es idéntica al mandato **list permanent-virtual-circuit**.

FR 1>list virtual-circuits

Circuit Number	Circuit Name	Options	Type/State	Frames Transmitted	Frames Received
16	Unassigned	F	P/I	0	0
17	Unassigned	F H	P/I	0	0
23	To-Kitty	F H	P/I	0	0

Circuit type: O - Orphan P - PVC S - SVC
 Circuit state: A - Active I - Inactive R - Removed C - Congested
 R - Required G - Required and belongs to a PVC group
 F - circuit is fragmentation capable
 c - Data compression capable but not operational
 C - Data compression capable and operational
 d - CDMF DES data encryption capable but not operational
 D - CDMF DES data encryption capable and operational
 t - 3DES data encryption capable but not operational
 T - 3DES data encryption capable and operational
 V - circuit is voice forwarding enabled

voice-forwarding-circuits

Visualiza todos los PVC que se han definido con posibilidad de reenviar paquetes de voz.

FR 2>list voice-forwarding-circuits

Circuit Name	Circuit Number	Forwarding Network	Forwarding Circuit
circ16	16	2	17
circ17	17	2	16

LLC

Utilice el mandato **LLC** para acceder al indicador de supervisión LLC. Los mandatos LLC se entran en este nuevo indicador. Consulte la sección “Mandatos de supervisión LLC” en la página 255 para ver una explicación de cada uno de estos mandatos.

Sintaxis:

llc

Nota: El mandato LLC sólo está soportado si APPN está en la carga de software.

Notrace

Utilice el mandato **notrace** para inhabilitar el rastreo de paquetes para circuitos individuales o en toda la interfaz. Este mandato puede utilizarse como filtro cuando es necesario rastrear circuitos o interfaces específicos. El valor por omisión es rastrear todos los circuitos.

Sintaxis:

```
notrace                númerocircuito
                        nombrecircuito
                        all
```

Ejemplo:

```
notrace 16
    Disables packet tracing on circuit (PVC or SVC) with DLCI 16.
notrace circuit phoenix
    Disables packet tracing on circuit (PVC or SVC) named phoenix.
notrace circuit all
    Disables packet tracing on all circuits on this interface.
```

Set

Utilice el mandato **set** para establecer los valores para la Velocidad de información confirmada (CIR), la Velocidad de ráfaga confirmada y la Velocidad de exceso de ráfaga para el VC especificado. También puede establecer valores para las velocidades de ajuste de IR.

Los cambios realizados con este mandato no afectan a los datos de configuración. Sólo surten efecto hasta que se reinicia el direccionador.

Sintaxis:

```
set                    circuit . . .
                        ir-adjustment . . .
```

circuit *númerocircuito o nombre volcir valbc valbe*

Establece los valores para la Velocidad de información confirmada (CIR), la Velocidad de ráfaga confirmada y la Velocidad de exceso de ráfaga para el VC especificado y puede utilizarse para cambiar la CIR, Bc y Be de salida operativa para un PVC o un SVC activo.

Ejemplo:

Supervisión de interfaces Frame Relay

```
set circuit  
Circuit number [16]?  
Committed Information Rate (CIR) in bps [1200]?  
Committed Burst Size (Bc) in bits [1200]?  
Excess Burst Size (Be) in bits [56000]?
```

Circuit Number

Indica el número del circuito en el rango de 16 a 1007.

Committed Information Rate

Indica la velocidad de información confirmada (CIR). La CIR puede ser 0 o un valor en el rango de 300 bps a 2 048 000 bps. El valor por omisión es 64 kbps. Para obtener más información, consulte la sección “Velocidad de información confirmada (CIR)” en la página 543.

Committed Burst Size

La cantidad máxima de datos en bits que el direccionador enviará durante una medición de intervalo igual al tamaño de ráfaga confirmado (Bc) / CIR segundos. El rango es de 300 a 2 048 000 bits. El valor por omisión es 64 Kb.

Nota: Si la CIR se configura como 0, el tamaño de ráfaga confirmada se establece en 0 y no se solicita ningún valor. Para obtener información adicional, consulte la sección “Tamaño de ráfaga confirmado (Bc)” en la página 544.

Excess Burst Size

La cantidad máxima de datos no confirmados en bits que sobrepasan el tamaño de ráfaga confirmado que el direccionador intenta entregar durante un intervalo de medición igual a (Tamaño de ráfaga confirmado/CIR) segundos. El rango es de 0 a 2 048 000 bits. El valor por omisión es 0. Para obtener información adicional, consulte la sección “Tamaño de exceso de ráfaga (Be)” en la página 544.

ir-adjustment %-incremento %-decremento IR-mínima

Establece la velocidad mínima de información (IR) y los porcentajes para incrementar o decrementar la IR en respuesta de la congestión de la red.

Nota: El mandato **set ir-adjustment** de Talk 5 no es aplicable para subinterfaces FR.

La IR mínima, expresada como porcentaje de CIR, es el límite inferior de la velocidad de información. El porcentaje mínimo es 1 y el porcentaje máximo es 100. El valor por omisión es 25.

Cuando desaparece la congestión de la red, la velocidad de información aumenta gradualmente en el porcentaje de incremento de ajuste de IR hasta que se alcanza la velocidad máxima de información. El porcentaje mínimo es 1 y el porcentaje máximo es 100. El valor por omisión es 12.

Cuando se produce una congestión de la red, la velocidad de información se reduce en el porcentaje de decremento del ajuste de IR cada vez que se recibe una trama que contiene una BECN hasta que se alcanza la velocidad mínima de información. El porcentaje mínimo es 1 y el porcentaje máximo es 100. El valor por omisión es 25.

Ejemplo:

```
set ir-adjustment
  IR adjustment % increment [12]?
  IR adjustment % decrement [25]?
  Minimum IR as % of CIR [25]?
```

Trace

Utilice el mandato **Trace** para habilitar el rastreo de paquetes para circuitos individuales o para toda la interfaz y para listar la posibilidad de rastreo de todos los circuitos de esta interfaz. Este mandato puede utilizarse como filtro cuando es necesario rastrear circuitos o interfaces específicos. El valor por omisión es rastrear todos los circuitos.

Sintaxis:

```
trace                all
                    nombrecircuito
                    númerocircuito
                    list
```

Ejemplo:

```
trace 16
  Enables packet tracing on circuit (PVC or SVC) with DLCI 16.
trace circuit phoenix
  Enables packet tracing on circuit (PVC or SVC) named phoenix.
trace circuit all
  Enables packet tracing on all circuits on this interface.
```

```
trace list
The following circuits are available for packet trace
Circuit Name                Circuit Number
-----
Unassigned                  16
phoenix                     25
jetsam                      0
```

Lists the packet tracing capability of all circuits on this interface.

Interfaces Frame Relay y mandato interface de GWCON

Aunque las interfaces Frame Relay tienen un proceso para la supervisión, el direccionador también visualiza estadísticas completas para las interfaces instaladas cuando se utiliza el mandato **interface** desde el entorno GWCON. (Para obtener más información sobre el mandato **interface**, consulte la sección "Capítulo 8. El proceso de operación/supervisión (GWCON - Talk 5) y sus mandatos" en la página 117)

Estadísticas visualizadas para las interfaces Frame Relay

Se visualizan estadísticas similares a las siguientes cuando se ejecuta el mandato **interface** desde el entorno GWCON para interfaces Frame Relay. La pantalla real variará dependiendo del tipo de adaptador, por ejemplo, X.21, V.35 o HSSI.

Si se han configurado subinterfaces FR, las estadísticas GWCON y los mandatos de error para la interfaz base FR visualizarán las cuentas acumuladas de todos los circuitos de la interfaz base FR y todas las subinterfaces asociadas. Para una subinterfaz, estos mandatos sólo listarán cuentas para los circuitos definidos para la subinterfaz.

```
+interface 10
Nt Nt' Interface Slot-Port Self-Test Self-Test Maintenance
10 10 FR/0 Slot: 8 Port: 0 Passed Failed Failed
                2                1                0
```

Supervisión de interfaces Frame Relay

Frame Relay MAC/data-link on V.35/V.36 interface

Adapter cable: V.35 DTE

V.24 circuit: 105 106 107 108 109
Nicknames: RTS CTS DSR DTR DCD
PUB 41450: CA CB CC CD CF
State: ON ON ON ON ON

Line speed: 64.000 Kbps
Last port reset: 1 hour, 20 minutes, 42 seconds ago

Input frame errors:
CRC error 0 alignment (byte length) 0
missed frame 182 too long (> 2062 bytes) 0
aborted frame 0 DMA/FIFO overrun 0
Output frame counters:
DMA/FIFO underrun errors 0 Output aborts sent 0

Nt Indica el número de interfaz tal como lo ha asignado el software durante la configuración inicial.

Nt' Indica el número de interfaz, tal como lo ha asignado el software durante la configuración inicial.

Nota: Para interfaces de circuitos de marcación FR, Nt' es diferente de Nt. Nt' indica la interfaz base (RDSI) en la que se ejecuta el circuito de marcación.

Interface

Indica el tipo de interfaz y su número de instancia. Frame relay tiene una designación FR.

Slot Indica la ranura de la interfaz que ejecuta Frame Relay

Port Indica el puerto de la interfaz que ejecuta Frame Relay

Self-test Passed

Indica el número total de veces que la interfaz Frame Relay ha pasado la autoprueba.

Self-test Failed

Indica el número total de veces que la interfaz Frame Relay no ha pasado la autoprueba.

Maintenance Failed

Indica el número total de veces que la interfaz no ha podido comunicarse con la gestión de Frame Relay.

V.24 circuit, Nicknames, and State

Los circuitos, señales de control, asignaciones de patillas y su estado (ON u OFF).

Nota: El símbolo - - - en la salida de supervisión indica que el valor o el estado es desconocido.

Line speed

La velocidad de reloj de transmisión.

Last port reset

El período de tiempo desde el último restablecimiento de puerto.

Input frame errors:

CRC error

El número de paquetes recibidos que contenían errores de suma de comprobación y como consecuencia de ellos se han eliminado.

Supervisión de interfaces Frame Relay

Alignment

El número de paquetes recibidos que no eran un múltiplo par de 8 bits de longitud y como consecuencia de ellos se han eliminado.

Too long

El número de paquetes mayores que el tamaño configurado y como resultado de ello se han eliminado.

Aborted frame

El número de paquetes recibidos que se han cancelado anormalmente por el emisor o un error de línea.

DMA/FIFO overrun

El número de veces que la interfaz serie no ha podido enviar datos con la suficiente rapidez a la memoria del almacenamiento intermedio de paquetes del sistema para recibirlos de la red.

Missed frame

Cuando una trama llega al dispositivo y no hay ningún almacenamiento intermedio disponible, el hardware elimina la trama e incrementa el contador de tramas que faltan.

L & F bits not set

En interfaces serie, el hardware establece información de descriptor de entrada para las tramas que llegan. Si el almacenamiento intermedio puede aceptar la trama completa en la llegada, el hardware establece el primer y último bit de la trama, lo que indica que el almacenamiento intermedio ha aceptado toda la trama. Si no se establece alguno de estos bits, se elimina el paquete, se incrementa el contador L & F bits not set y se borra el almacenamiento intermedio para reutilización. Este contador no se visualizará para todos los tipos de adaptador.

Nota: No es probable que el contador L & F bits not set se vea afectado por el tráfico.

Output frame counters:

DMA/FIFO underrun errors

El número de veces que la interfaz serie no ha podido recuperar datos con la suficiente rapidez de la memoria del almacenamiento intermedio de paquetes del sistema para transmitirlos a la red.

Output aborts sent

El número de transmisiones que se han cancelado anormalmente como petición del software de nivel superior.

Se visualizan estadísticas similares a las siguientes para los circuitos de marcación Frame Relay cuando se ejecuta el mandato **interface** desde el entorno GWCON:

+interface 3

Nt	Nt'	Interface	Passed	Self-Test Failed	Self-Test Failed	Maintenance Failed
3	2	FR/1		1	0	0

Frame Relay MAC/data-link on ISDN Primary Rate interface

Soporte para la reconfiguración dinámica de Frame Relay

Esta sección describe la reconfiguración dinámica (DR) en la medida en que afecta a los mandatos Talk 6 y Talk 5.

Supervisión de interfaces Frame Relay

Delete Interface de CONFIG (Talk 6)

Frame Relay soporta el mandato **delete interface** de CONFIG (Talk 6) sin ninguna restricción.

Activate Interface de GWCON (Talk 5)

Frame Relay soporta el mandato **activate interface** de GWCON (Talk 5) con las consideraciones siguientes:

- No puede activar una interfaz de circuito de marcación Frame Relay a menos que la red base del circuito de marcación ya esté activada.
- No puede activar un circuito de marcación Frame Relay a menos que su red base se haya establecido para RDSI canalizada.
- El mandato **activate** para un circuito de marcación Frame Relay fallará si el tamaño de trama, la cabecera MAC o la cola necesarios para la interfaz de repuesto son mayores que los valores de estos parámetros configurados para otros circuitos de marcación que ya están asignados a la red base.

Los cambios en la configuración de Frame Relay se activan automáticamente excepto los siguientes:

Los mandatos cuyos cambios no se activan con el mandato activate interface de GWCON (Talk 5)

CONFIG, net, enable compression

Nota: Si todavía no se ha activado la compresión de datos en otra interfaz Frame Relay, no puede habilitarse cuando se active la interfaz.

Reset Interface de GWCON (Talk 5)

Frame Relay soporta el mandato **reset interface** de GWCON (Talk 5) con las consideraciones siguientes:

- Un circuito de marcación Frame Relay no puede restablecerse si se ha cambiado alguno de los parámetros del circuito de marcación que se configuran en el indicador `Dial Circuit config`.
- No puede restablecerse una interfaz Frame Relay que se utiliza para la Redirección WAN

Los cambios en la configuración de Frame Relay se activan automáticamente excepto los siguientes:

Mandatos cuyos cambios no se activan por el mandato reset interface de GWCON (Talk 5)
--

CONFIG, net, set frame-size

Nota: El usuario no puede aumentar el tamaño de trama.

CONFIG, net, enable compression

Nota: El usuario no puede habilitar la compresión en la interfaz si ya no está habilitada o habilitada en otra interfaz Frame Relay.

Mandatos de cambio temporal de GWCON (Talk 5)

Frame Relay soporta los mandatos GWCON siguientes que cambian temporalmente el estado operativo del dispositivo. Estos cambios se pierden cuando se vuelve a cargar o se reinicia el dispositivo o cuando se ejecuta algún mandato reconfigurable dinámicamente.

Supervisión de interfaces Frame Relay

Mandatos
GWCON, net, set circuit
GWCON, net, set ir-adjustment
GWCON, net, enable cir-monitor
GWCON, net, enable cllm
GWCON, net, enable congestion-monitor
GWCON, net, enable notify-fecn-source
GWCON, net, enable throttle-transmit-on-fecn
GWCON, net, disable cir-monitor
GWCON, net, disable cllm
GWCON, net, disable congestion-monitor
GWCON, net, disable notify-fecn-source
GWCON, net, disable throttle-transmit-on-fecn

Supervisión de interfaces Frame Relay

Capítulo 43. Utilización de interfaces de Point-to-Point Protocol

Este capítulo describe cómo utilizar Point-to-Point Protocol para las interfaces del dispositivo. Las secciones de este capítulo son:

- “Visión general de PPP”
- “Link Control Protocol (LCP) de PPP” en la página 624
- “Protocolos de autenticación de PPP” en la página 628
- “Utilización de AAA con PPP” en la página 633
- “Network Control Protocol de PPP” en la página 633
- “Utilización y configuración de conexiones virtuales” en la página 636

Consulte las secciones “Capítulo 45. Utilización de Multilink PPP Protocol” en la página 691 y “Capítulo 46. Configuración y supervisión de Multilink PPP Protocol (MP)” en la página 697 para obtener información sobre la utilización de Multilink PPP Protocol

Visión general de PPP

PPP proporciona un método para transmitir datagramas de protocolo en la Capa de enlace de datos a través de enlaces de punto a punto serie. PPP proporciona los servicios siguientes:

- Link Control Protocol (LCP) para establecer, configurar y probar la conexión del enlace.
- Un protocolo de encapsulación para encapsular los datagramas del protocolo a través de enlaces punto a punto serie.
- Protocolos de autenticación (AP) para validar la identidad de una unidad igual (remota) y someter su propia identidad al igual para validación.
- Protocolos Network Control Protocol (NCP) para establecer y configurar distintos protocolos de capa de red. PPP permite la utilización de múltiples protocolos de capa de red.

La Figura 45 en la página 622 muestra algunos ejemplos de enlaces serie de punto a punto.

Utilización de PPP

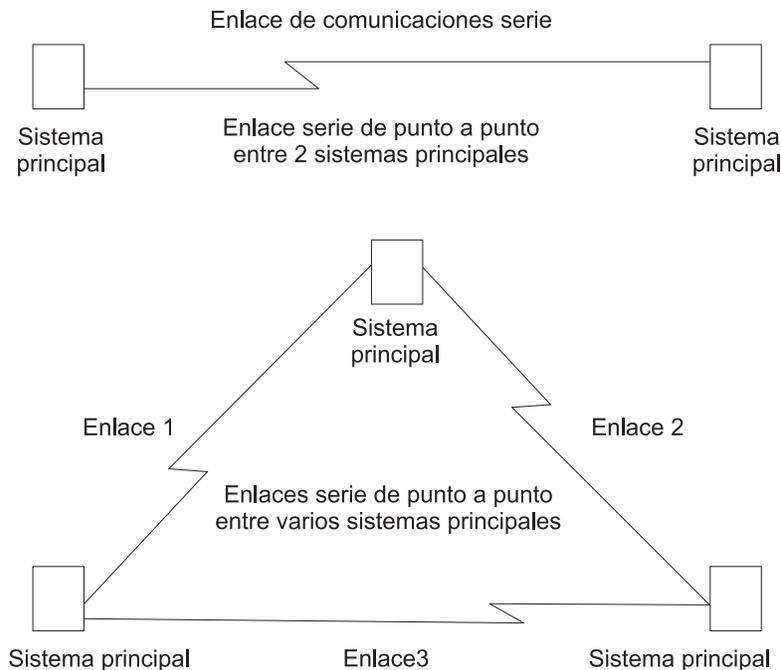


Figura 45. Ejemplos de enlaces de punto a punto

Actualmente PPP soporta los siguientes protocolos de control:

- AppleTalk Control Protocol (ATCP)
- DECnet Protocol Control Protocol (DNCP)
- Banyan VINES Control Protocol (BVCP)
- Protocolos Bridging (BCP, NBSP y NBFSP)
- Internet Protocol Control Protocol (IPCP)
- Internet Protocol Version 6 Control Protocol (IPv6CP)
- IPX Control Protocol (IPXCP)
- APPN HPR Control Protocol (APPN HPRCP)
- APPN ISR Control Protocol (APPN ISRCP)
- OSI Control Protocol (OSICP)

Cada extremo empieza por enviar paquetes LCP para configurar y probar el enlace de datos. Después de establecer el enlace, PPP envía paquetes NCP para elegir y configurar uno o varios protocolos de capa de red. Después de configurar los protocolos de capa de red, pueden enviarse datagramas de cada capa de red a través del enlace. Las secciones siguientes explican estos conceptos con más detalle.

Estructura de trama de capa de enlace de datos PPP

PPP transmite tramas de datos que tienen la misma estructura que las tramas High-level Data Link Control (HDLC). PPP utiliza un método de transmisión orientado a bytes con un formato de una sola trama para todos los datos e intercambios de control. La Figura 46 en la página 623 ilustra la estructura de trama PPP y le sigue una descripción detallada de cada campo.

Dist.	Direcc.	Control	Protocolo	Información	FCS	Dist.
8 bits	8 bits	8 bits	16 bits	variable	16 bits	8 bits

Figura 46. Estructura de trama PPP

Campos de distintivo

El campo de distintivo inicia y finaliza cada trama con el patrón exclusivo 01111110. Generalmente, un solo distintivo finaliza una trama e inicia la siguiente. El receptor conectado al enlace continuamente busca la secuencia del distintivo para sincronizar el inicio de la trama siguiente.

Campo de dirección

El campo de dirección consta de un solo octeto (8 bits) y contiene la secuencia binaria 11111111 (0xff hexadecimal). Esto se conoce como la Dirección de todas las estaciones. PPP no asigna direcciones de estaciones individuales.

Campo de control

El campo de control tiene un solo octeto y contiene la secuencia binaria 00000011 (0x03 hexadecimal). Esta secuencia identifica el mandato Unnumbered Information (UI) con el bit P/F establecido en cero.

Campo de protocolo

El campo de protocolo se define por PPP. El campo consta de 2 octetos (16 bits) y su valor identifica el datagrama de protocolo encapsulado en el campo de información de la trama.

Los valores del campo de protocolo que están en el rango de '0xC000' a '0xFFFF' indican datos de la Capa 3 (datagramas de protocolo) como, por ejemplo, LCP, PAP, CHAP,

Campo de información

El campo de información contiene el datagrama para el protocolo especificado en el campo de protocolo. Tiene cero o más octetos.

Cuando el tipo de protocolo es LCP, se encapsula exactamente un paquete LCP en el campo de información de las tramas de Capa de enlace de datos PPP.

Campo de secuencia de comprobación de tramas (FCS)

El campo de secuencia de comprobación de tramas es una comprobación de redundancia cíclica de 16 bits (CRC).

Los enlaces PPP pueden negociar la utilización de diversas opciones que pueden modificar el formato básico de la trama; la descripción de más abajo se aplica al formato de trama anterior a cualquiera de esas modificaciones. Los paquetes LCP de PPP siempre se envían en este formato también, sin tener en cuenta las opciones negociadas, de modo que los paquetes LCP pueden reconocerse incluso cuando se pierde la sincronización en la línea.

El direccionador soporta dos opciones: Compresión de campo de dirección y de control (ACFC) y compresión de campo de protocolo (PFC). Estas opciones se describen con detalle en una sección posterior.

Link Control Protocol (LCP) de PPP

Link Control Protocol (LCP) de PPP establece, configura, mantiene y termina el enlace de punto a punto. Este proceso se lleva a cabo en cuatro fases:

1. Antes de intercambiar cualquier datagrama de capa de red, PPP abre primero la conexión a través de un intercambio de paquetes de configuración LCP. Como parte de este proceso de negociación, los procesos PPP de cada extremo del enlace se ponen de acuerdo sobre diversos parámetros básicos de nivel de enlace como, por ejemplo, el tamaño máximo de paquete que puede transferirse y si los extremos deben utilizar un mecanismo de autenticación para identificarse a sí mismos con sus iguales antes de transportar el tráfico de red.

Si esta negociación no es satisfactoria, se considera que el enlace está “desactivado” y que no es capaz de transportar ningún tráfico de red. Si la negociación es satisfactoria, LCP pasa a un estado “Abierto” y PPP pasa a la fase siguiente.

2. Después de que LCP alcance satisfactoriamente un estado Abierto, el siguiente paso del establecimiento del enlace es realizar la autenticación en la que cada extremo del enlace se identifica a sí mismo en el otro extremo utilizando el “protocolo de autenticación” que el otro extremo ha impuesto como parte de la negociación LCP.

Si falla la autenticación, se pone la marca de “desactivado” en el enlace y no puede transportar ningún tráfico de red. Si la autenticación es satisfactoria o si no es necesaria, el enlace PPP pasa a la fase siguiente.

3. Después de negociar la autenticación, los iguales negocian el cifrado para el enlace. Después de completar la fase de autenticación, el direccionador negocia la utilización del cifrado utilizando paquetes de Encryption Control Protocol (ECP) donde cada extremo del enlace negocia el algoritmo de cifrado que se utilizará para cifrar los datos a través de este enlace PPP. Si ECP no ha alcanzado el estado “Abierto”, el enlace se marca como “desactivado” y no puede transportar ningún tráfico de red. Si ECP alcanza satisfactoriamente el estado “Abierto” o si no es necesario el cifrado, el enlace PPP pasa a la fase siguiente, la negociación NCP (excepto ECP, que técnicamente también es un NCP). En este momento, se considera que el enlace está “abierto” o “activado”, aunque todavía no puede transportar datagramas de protocolo de capa 3.

4. Una vez que el enlace está abierto, el direccionador negocia la utilización de varios protocolos de capa 3 (por ejemplo, IP, IPX, DECnet, Banyan Vines) utilizando paquetes de Network Control Protocol (NCP). Cada protocolo de capa 3 tiene su propio protocolo de control de red asociado. Por ejemplo, IP tiene IPCP e IPX tiene IPXCP. El formato básico y los mecanismos para todos estos paquetes NCP es el mismo para todos los protocolos y es, básicamente, un superconjunto de los mecanismos LCP, tal como se describe más adelante en esta sección.

Cada protocolo de capa 3 se negocia independientemente. Cuando un NCP negocia satisfactoriamente, el enlace se “activa” para el tráfico de este protocolo. Como con LCP, puede intercambiarse la información de configuración como parte de esta negociación; por ejemplo, IPCP puede intercambiar direcciones IP o negociar la utilización de la “compresión de cabecera IP Van Jacobson”.

Como con LCP, es posible que un NCP no pueda negociar satisfactoriamente con su igual. Esto puede producirse porque el igual no soporta un protocolo en particular o porque alguna opción de configuración no es aceptable. Si un NCP no puede alcanzar el estado “Abierto”, no se pueden intercambiar paquetes de

protocolo de capa 3 para ese protocolo aunque otros protocolos de capa 3 estén pasando tráfico satisfactoriamente a través del enlace PPP.

5. Finalmente, LCP tiene la posibilidad de terminar el enlace en cualquier momento. Normalmente, esto se realiza a petición del usuario pero puede producirse por otras razones como: un cierre administrativo del enlace, la caducidad del temporizador de desocupado o cuando no se puede volver a autenticar en una cuestión de la identidad CHAP.

Para ver detalles completos acerca de LCP de PPP, la autenticación y los mecanismos generales de negociación de NCP, consulte los RFC 1331, 1334, 1570 y 1661.

Paquetes LCP

Los paquetes LCP se utilizan para establecer y gestionar un enlace PPP y pueden dividirse en tres categorías:

- Los *paquetes de establecimiento de enlace* que intercambian información de configuración y establecen el enlace.
- Los *paquetes de terminación de enlace* que cierran el enlace o señalan que un enlace no está aceptando conexiones en un momento determinado. También pueden utilizarse para señalar que no se puede reconocer un protocolo en particular (por ejemplo, durante las negociaciones NCP).
- Los *paquetes de mantenimiento de enlace* que supervisan y depuran un enlace.

Se encapsula un paquete LCP exactamente en el campo de información de las tramas de Capa de enlace de datos PPP. En el caso de paquetes LCP, el campo de protocolo indica "Link Control Protocol" (C021 hexadecimal). La Figura 47 ilustra la estructura del paquete LCP y va seguida de una descripción detallada de cada campo.

Cód.	Identific.	Longit.	Datos (opc.)
------	------------	---------	--------------

Figura 47. Estructura de trama LCP (en el campo de información PPP)

Código

El campo de código tiene un octeto de longitud e identifica el tipo de paquete LCP. Los códigos de la Tabla 77 distinguen los tipos de paquetes. Se describen con más detalle en secciones posteriores.

Tabla 77. Códigos de paquetes LCP

Código	Tipo de paquete
1	Petición de configuración (establecimiento de enlace)
2	Reconocimiento de configuración (establecimiento de enlace)
3	No reconocimiento de configuración (establecimiento de enlace)
4	Rechazo de configuración (establecimiento de enlace)
5	Petición de terminación (terminación de enlace)
6	Reconocimiento de terminación (terminación de enlace)
7	Rechazo de código (establecimiento de enlace)
8	Rechazo de protocolo (establecimiento de enlace)
9	Petición de eco (mantenimiento de enlace)
10	Respuesta de eco (mantenimiento de enlace)
11	Petición de rechazo (mantenimiento de enlace)

Utilización de PPP

Identificador

El campo de identificador tiene un octeto de longitud y se utiliza para emparejar las peticiones de paquetes con las respuestas.

Longitud

El campo de longitud tiene dos octetos de longitud e indica la longitud total (es decir, incluyendo todos los campos) del paquete LCP.

Datos (opción)

El campo de datos tiene cero o más octetos, tal como indica el campo de longitud. El formato de este campo se determina por el código.

Los paquetes NCP están estructurados idénticamente a los paquetes LCP y se distinguen por tener valores diferentes de "Protocolo" PPP. Cada tipo de paquete LCP (diferenciado por el campo de código) tiene el mismo significado para cada NCP, aunque puede que un NCP individual no implemente todos los tipos posibles de paquetes LCP. Normalmente, los NCP implementan todos los paquetes del tipo de establecimiento de enlace que el LCP define. Pueden implementar algunos de los tipos adicionales de paquetes LCP y también pueden definir tipos de paquetes diferentes, además de los que LCP utiliza. A diferencia de los paquetes LCP, la estructura de una trama NCP puede modificarse de acuerdo a las opciones negociadas por LCP durante la fase de establecimiento del enlace.

Paquetes de establecimiento de enlace

Los paquetes de establecimiento de enlace establecen y configuran un enlace de punto a punto incluyendo los tipos de paquetes siguientes:

Petición de configuración

El campo de código de paquete LCP se establece en 1. LCP transmite este tipo de paquete cuando desea abrir un enlace de punto a punto. En la recepción de una Petición de configuración, la entidad LCP de una estación igual envía una respuesta adecuada, dependiendo de si está preparada para procesar paquetes.

Reconocimiento de configuración

El campo de código de paquete LCP se establece en 2. El igual transmite este tipo de paquete cuando se pueden aceptar todas las opciones de configuración de un paquete de Petición de configuración. En la recepción del Reconocimiento de configuración (ack), la estación de origen comprueba el campo de identificador. Este campo debe coincidir con el de la Petición de configuración que se ha transmitido en último lugar o el paquete no es válido.

Ambos extremos envían una Petición de configuración y ambos extremos deben recibir un Reconocimiento de configuración antes de que se abra el enlace. Las opciones negociadas para una dirección pueden diferir de las negociadas para la otra dirección. No hay ninguna relación "maestro-esclavo". En su lugar, cada extremo funciona simétricamente.

No reconocimiento de configuración

El campo de código del paquete LCP se establece en 3. El igual transmite este tipo de paquete cuando no se pueden aceptar parte de las opciones de configuración de un paquete Petición de configuración. El campo de identificador se copia de la Petición de configuración y el campo de datos (opción) se rellena con las opciones de configuración no aceptables recibidas. El campo de identificador debe coincidir con el de la Petición de configuración que se ha transmitido por última vez o el paquete es no válido y se elimina.

Cuando el originador recibe un paquete de No reconocimiento de configuración, se envía un nuevo paquete de Petición de configuración que incluye las opciones de configuración modificadas y aceptables.

Rechazo de configuración

El campo de código del paquete LCP se establece en 4. El igual transmite este tipo de paquete cuando parte de las opciones de configuración de un paquete Petición de configuración no son aceptables. El campo de identificador se copia de la Petición de configuración y el campo de datos (opción) se rellena con las opciones de configuración no aceptables recibidas. El campo de identificador debe coincidir con el de la Petición de configuración que se ha transmitido por última vez o el paquete es no válido y se elimina.

Cuando el originador recibe un paquete de Rechazo de configuración, se envía un nuevo paquete de Petición de configuración que no incluye ninguna de las opciones de configuración recibidas en el paquete de Rechazo de configuración.

Rechazo de código

El campo de código del paquete LCP se establece en 7. La transmisión de este tipo de paquete indica que el campo de "código" de un paquete recibido no se reconoce como un valor válido. Aunque esto puede indicar un error, también puede indicar que el igual no implementa alguna de las características que se están intentando utilizar.

Rechazo de protocolo

El campo de código del paquete LCP se establece en 8. La transmisión de este tipo de paquete indica que se ha recibido una trama PPP que contiene un protocolo no soportado o no conocido (no se ha reconocido el campo de "protocolo" de PPP para algún paquete). Normalmente, esto se produce si se intenta negociar algún NCP para un protocolo que el otro extremo no soporta. Por ejemplo, si DECnet CP (DNCP) envía una Petición de configuración y el otro extremo no reconoce DECnet, éste responde con un Rechazo de protocolo LCP en DNCP. En la recepción de un paquete de Rechazo de protocolo, el enlace deja de transmitir el protocolo incorrecto.

Nota: Los tipos y estructuras de paquete NCP son iguales a LCP, aunque hay unos cuantos campos de "código" adicionales que se asocian con algunos NCP.

Paquetes de terminación de enlace

Los paquetes de terminación de enlace terminan un enlace e incluyen los tipos de paquetes siguientes:

Petición de terminación

El campo de código del paquete LCP se establece en 5. LCP transmite este tipo de paquete cuando es necesario cerrar un enlace de punto a punto. Se envían estos paquetes hasta que se devuelve un paquete de Reconocimiento de terminación, o hasta que se excede el contador de reintentos mientras se espera un reconocimiento.

Reconocimiento de terminación

El campo de código del paquete LCP se establece en 6. En la recepción de un paquete de Petición de terminación, debe transmitirse este tipo de paquete con el campo de código establecido en 6. La recepción de un paquete de Reconocimiento de terminación que no se esperaba indica que se ha cerrado el enlace.

Utilización de PPP

Paquetes de mantenimiento de enlace

Los paquetes de mantenimiento de enlace gestionan y depuran un enlace e incluyen los tipos de paquetes siguientes:

Petición de eco y Respuesta de eco

Los campos de código de paquetes LCP se establecen en 9 y 10 respectivamente. LCP transmite estos tipos de paquetes para proporcionar un mecanismo de bucle de retorno de Capa de enlace de datos para ambas direcciones del enlace. Esta característica es útil, por ejemplo, para determinar la calidad del enlace en la depuración de un enlace anómalo. Estos paquetes sólo se envían cuando el enlace está en estado abierto.

Petición de eliminación

El campo de código del paquete LCP se establece en 11. LCP transmite este tipo de paquete para proporcionar un destino para los datos en la prueba de Capa de enlace de datos. Un igual que recibe una Petición de eliminación **debe** eliminar el paquete. Es útil en la depuración de un enlace. Estos paquetes sólo se envían cuando el enlace está en estado abierto.

Protocolos de autenticación de PPP

Los protocolos de autenticación de PPP proporcionan una forma de seguridad entre dos nodos conectados a través de un enlace PPP. Si es necesaria la autenticación en una máquina, inmediatamente después de que dos máquinas negocien satisfactoriamente la utilización del enlace en la capa LCP (se intercambian paquetes LCP hasta que LCP llega al estado “abierto”), pasan a una fase de “autenticación” en la que intercambian paquetes de autenticación. Una máquina no puede transportar paquetes de datos de red ni negociar la utilización de un protocolo de red (tráfico NCP) hasta que la negociación de autenticación se completa satisfactoriamente.

Se utilizan diferentes protocolos de autenticación: Password Authentication Protocol (PAP) y Challenge/Handshake Authentication Protocol (CHAP). También está disponible Microsoft PPP CHAP (MS-CHAP) para autenticar las estaciones de trabajo Windows y los direccionadores iguales. PAP y CHAP se describen con detalle en RFC 1334 y brevemente más adelante en esta sección. MS-CHAP se describe en RFC 1994.

En puertos de acceso de marcación remotos, está disponible un tercer protocolo de autenticación. Se trata de Shiva Password Authentication Protocol (SPAP), que es un protocolo propiedad de Shiva. Consulte la sección “Shiva Password Authentication Protocol (SPAP)” en la página 630 para obtener más información.

Se determina si una máquina necesita que el otro extremo se autentique a sí mismo (y si procede, con qué protocolo) durante la fase de negociación de LCP. La autenticación podría considerarse que ha “fallado” incluso en la fase de establecimiento de enlace (negociación LCP), si un extremo no sabe cómo utilizar o rechaza el protocolo de autenticación que el otro extremo necesita.

Cada extremo de un enlace establece sus propios requisitos de cómo desea que el otro extremo se autentique a sí mismo. Por ejemplo, si tenemos dos direccionadores “A” y “B”, conectados a través de un enlace PPP, la parte A puede necesitar que B se autentique a sí mismo en A utilizando PAP, y la parte B puede necesitar que A se identifique a sí mismo utilizando CHAP. Es válido que un extremo necesite autenticación mientras que el otro no necesite ninguna.

Además de la autenticación inicial durante el establecimiento del enlace, puede que con algunos protocolos un autenticador pida que el igual restablezca sus credenciales periódicamente. Con CHAP, por ejemplo, el autenticador puede emitir una cuestión de la identidad en cualquier momento y el igual debe responder satisfactoriamente o perder el enlace.

Si hay más de un protocolo de autenticación habilitado en un enlace, en principio el direccionador intenta utilizarlos siguiendo el orden de prioridad siguiente:

1. MS-CHAP
2. CHAP
3. PAP
4. SPAP

Nota: SPAP sólo está disponible en interfaces que tienen configurados circuitos de marcación de entrada IBM DIAL.

Si la parte remota responde a la petición de autenticación con NAK (no reconocimiento) y sugiere una alternativa, el direccionador utiliza la alternativa, siempre que esté habilitada en el enlace. Si la parte remota continúa respondiendo a las sugerencias del direccionador con NAK pero no proporciona ninguna alternativa que el direccionador tenga habilitada, se termina el enlace.

Password Authentication Protocol (PAP)

Password Authentication Protocol (PAP) proporciona un método simple para que el igual establezca su identidad utilizando un acuerdo bilateral. Esto sólo se realiza en el establecimiento inicial del enlace. Después del establecimiento del enlace, el igual envía un par ID/contraseña al autenticador hasta que se reconoce la autenticación o se termina la conexión. Las contraseñas se envían a través del circuito "sin condicionamientos" y no existe protección contra la reproducción ni contra las tentativas repetidas ni ataques de errores. El igual controla la frecuencia y el cronometraje de los intentos.

Challenge-Handshake Authentication Protocol (CHAP)

Challenge-Handshake Authentication Protocol (CHAP) se utiliza para verificar periódicamente la identidad del igual utilizando un acuerdo tridireccional. Esto se realiza en el establecimiento inicial del enlace y *puede* repetirse en cualquier momento después de que se haya establecido el enlace. Después del establecimiento inicial del enlace, el autenticador envía un mensaje de "cuestión de la identidad" al igual. El igual responde con un valor calculado utilizando una función "hash de una sola dirección". El autenticador comprueba la respuesta con su propio cálculo del valor de hash esperado. Si los valores coinciden, se reconoce la autenticación; de lo contrario, se termina la conexión.

Autenticación Microsoft CHAP de PPP (MS-CHAP)

MS-CHAP es una extensión de PPP CHAP que se utiliza para autenticar las estaciones de trabajo remotas Windows y los direccionadores iguales. Tanto MS-CHAP como CHAP utilizan el Link Control Protocol (LCP) de PPP para negociar el protocolo de autenticación deseado en una o en ambas direcciones; ambos utilizan el identificador de protocolo CHAP como protocolo PPP y cada protocolo utiliza una cuestión de la identidad aleatoria que está cifrada como parte de la respuesta.

Se puede utilizar MS-CHAP con la base de datos de la Lista local de usuarios PPP, pero **no** con el servidor de autenticación AAA externo que se describe en el capítulo "Utilización de autenticación local o remota" de la publicación *Utilización y*

Utilización de PPP

configuración de las características. Si piensa utilizar Microsoft PPP Encryption (MPPE) en una interfaz PPP, debe habilitar MS-CHAP en esa interfaz antes de configurar MPPE. Utilice el mandato **enable mschap** de talk 6 para habilitar MS-CHAP.

Shiva Password Authentication Protocol (SPAP)

Nota: SPAP sólo está disponible en interfaces que tienen configurados circuitos de marcación de entrada IBM DIAL.

Shiva Password Authentication Protocol (SPAP) proporciona un método sencillo para que el igual establezca su identidad utilizando un acuerdo bidireccional igual a PAP. Después de completar la fase de Establecimiento del enlace, el igual envía repetidamente un Id/Contraseña al autenticador hasta que se reconoce la autenticación, se termina la conexión o caduca un contador de reintentos.

SPAP es un protocolo de autenticación moderadamente potente que utiliza un algoritmo de cifrado de propiedad para la contraseña. Además de la autenticación, SPAP ofrece:

- La posibilidad de cambiar una contraseña.
- La posibilidad de que el direccionador envíe un mensaje de cabecera configurable que necesita reconocimiento del cliente después de la autenticación de la contraseña.
- La posibilidad de utilizar una llamada de retorno como característica adicional de seguridad.
- Conexiones virtuales.

Configuración de la autenticación PPP

Las secciones siguientes describen la configuración de las autenticaciones PPP para dos situaciones:

- La configuración del 2216 para autenticar un dispositivo remoto.
- La configuración del 2216 para que un dispositivo remoto lo autentifique.

Estas dos situaciones son independientes. Puede efectuar una o la otra.

Configuración de una interfaz PPP para autenticar un dispositivo remoto

Para autenticar un dispositivo remoto o un cliente de marcación de entrada:

1. Habilite la autenticación en la interfaz PPP
 - En el indicador `Config>`, entre el mandato **network** para seleccionar la interfaz PPP que se va a configurar.
 - En el indicador `PPP Config>`, habilite el protocolo de autenticación que desee utilizar.

Puede utilizar cualquiera de los protocolos siguientes:

- PAP
- MS-CHAP

Nota: MS-CHAP puede utilizar la base de datos local PPP para autenticar, pero no puede utilizar un servidor de autenticación.

- CHAP
- SPAP

Nota: SPAP sólo está disponible en interfaces que tienen configurados circuitos de marcación de entrada IBM DIAL.

2. Decida si desea autenticar localmente o a través de un servidor de autenticación.

- Para autenticar localmente, entre el nombre y contraseña en la base de datos de usuarios PPP.

En el indicador `Config>`, utilice el mandato **add ppp_user**. Consulte la sección “Add” en la página 77 para obtener más información.

Un 2216 mantiene una sola base de datos de usuarios PPP. Cuando el direccionador o dispositivo remoto envía su nombre y contraseña al dispositivo durante la fase de autenticación, el dispositivo comprueba si el nombre y contraseña están en la base de datos del usuario PPP.

- Para autenticar mediante un servidor de autenticación utilizando TACACS, TACACS+ o RADIUS, debe configurar el dispositivo para que llegue al servidor de autenticación y el nombre y la contraseña deben estar en la base de datos del servidor. Consulte la sección “Utilización de autenticación local o remota” de la publicación *Utilización y configuración de las características*.

Configuración de una interfaz PPP para que un dispositivo remoto la autentique

Para configurar el dispositivo para que un dispositivo remoto o cliente de marcación de entrada lo autentique, configure el nombre y la contraseña del dispositivo:

1. En el indicador `Config>`, seleccione la interfaz que está configurando utilizando el mandato **network**.
2. En el indicador `PPP Config>`, escriba el mandato **set name** y proporcione el nombre y la contraseña que el dispositivo utilizará para identificarse a sí mismo en el direccionador o dispositivo remoto durante la fase de autenticación.

Atención: No utilice los mandatos siguientes a menos que desee que el dispositivo realice la autenticación tal como se describe en la sección “Utilización de autenticación local o remota” de la publicación *Utilización y configuración de las características*.

- **enable pap**
- **enable chap**
- **enable spap**

Nota: SPAP sólo está disponible en interfaces que tienen configurados circuitos de marcación de entrada IBM DIAL.

- **enable mschap**

Configuración de llamada de retorno PPP

La llamada de retorno es una característica PPP asociada con las soluciones de marcación de entrada de un solo usuario. Intenta cumplir dos objetivos. Estos objetivos son:

- La llamada de retorno puede utilizarse como una forma de seguridad. Cuando se utiliza de esta manera, generalmente se hace referencia a la llamada de retorno como llamada de retorno necesaria. Cuando se negocia una llamada de retorno necesaria, se volverá a llamar al usuario a un número predeterminado. Sólo entonces se permitirá que el enlace PPP se active.
- También se puede implementar la llamada de retorno como una característica de ahorro de pago. Cuando se utiliza de esta manera, generalmente se hace referencia a la llamada de retorno como llamada de retorno voluntaria. A

Utilización de PPP

diferencia de la llamada de retorno necesaria, la llamada de retorno voluntaria se pide por el cliente. La función principal de la llamada de retorno voluntaria es facturar a la compañía que mantiene el Servidor DIAL, los cargos de la llamada en lugar de facturarlos al usuario.

La llamada de retorno sólo está soportada en circuitos de marcación de entrada a través de redes RDSI.

Ejemplo 1: Llamada de retorno necesaria habilitada

```
Config>add PPP
Enter user name: [ ]? nocalldback
Password:
Enter password again:
Is this a Single-User or a Network? (Single-User, Network): [Single-User]

IP address for user nocalldback [0.0.0.0]?
Enter HostName: [ ]?
Give 'nocalldback' default time allotted ? (Yes, No): [Yes]
Enable Callback for 'nocalldback' ? (Yes, No): [No] yes
Type of Callback (Roaming Callback, Required Callback): [Roaming Callback] Requ
Dialback number for this user [ ]? 555-1234
Will 'nocalldback' be able to dial-out ? (Yes, No): [No]

PPP User Name: nocalldback
Type: Single User
User IP Address: Interface Default
SubNetMask: 255.255.255.255
Hostname: <undefined>
Time-Allotted: Box Default
Call-Back Type: Required Callback
Phone Number: 543-3186
Dial-Out: Not Enabled
Encryption: Not Enabled

Is information correct? (Yes, No, Quit): [No] yes
```

Ejemplo 2: Llamada de retorno inhabilitada

```
Config>add PPP
Enter user name: [ ]? sallydoe
Password:
Enter password again:
Is this a Single-User or a Network? (Single-User, Network): [Single-User]

IP address for user nocalldback [0.0.0.0]?
Enter HostName: [ ]?
Give 'no callback' default time allotted ? (Yes, No): [Yes]
Enable Callback for 'no callback' ? (Yes, No): [No]
Will 'no callback' be able to dial-out ? (Yes, No): [No]

PPP User Name: no callback
Type: Single User
User IP Address: Interface Default
SubNetMask: 255.255.255.255
Hostname: <undefined>
Time-Allotted: Box Default
Call-Back Type: Not Enabled
Dial-Out: Not Enabled
Encryption: Not Enabled

Is information correct? (Yes, No, Quit): [No] yes
```

Ejemplo 3: Llamada de retorno voluntaria habilitada

```
Config>add PPP roaming_callback
Password:
Enter password again:
Is this a Single-User or a Network? (Single-User, Network): [Single-User]

IP address for user roaming_callback [0.0.0.0]?
Enter HostName: [ ]?
Give 'roaming_callback' default time allotted ? (Yes, No): [Yes]
Enable Callback for 'roaming_callback' ? (Yes, No): [No] yes
Type of Callback (Roaming Callback, Required Callback): [Roaming Callback]

Will 'roaming_callback' be able to dial-out ? (Yes, No): [No]n

PPP User Name: roaming_callback
Type: Single User
User IP Address: Interface Default
SubNetMask: 255.255.255.255
Hostname: <undefined>
```

Time-Allotted: Box Default
 Call-Back Type: Roaming Callback
 Dial-Out: Not Enabled
 Encryption: Not Enabled

Is information correct? (Yes, No, Quit): [No]yes

Utilización de AAA con PPP

Consulte las secciones “Utilización de autenticación local o remota” y “Configuración de autenticación” de la publicación *Utilización y configuración de las características* para obtener esta información.

Network Control Protocol de PPP

PPP tiene una familia de Network Control Protocol (NCP) para establecer y configurar diferentes protocolos de capa de red. Los NCP son los responsables de configurar, habilitar e inhabilitar los protocolos de capa de red en ambos extremos del enlace de punto a punto. Los paquetes NCP no pueden intercambiarse hasta que LCP ha abierto la conexión y el enlace alcanza el estado OPEN.

PPP da soporte a los Network Control Protocol siguientes:

- AppleTalk Control Protocol (ATCP)
- Banyan VINES Control Protocol (BVCP)
- Protocolos Bridging (BCP, NBCP y NBFCP),
- Callback Control Protocol
- DECnet Control Protocol (DNCP)
- IP Control Protocol (IPCP)
- IPv6 Control Protocol (IPv6CP)
- IPX Control Protocol (IPXCP)
- OSI Control Protocol (OSICP)
- APPN High Performance Routing Control Protocol (APPN HPRCP)
- APPN Intermediate Session Routing Control Protocol (APPN ISRCP)

AppleTalk Control Protocol

ATCP se especifica en la Petición de comentarios (RFC) 1378. La implementación que IBM hace de ATCP soporta la opción Dirección AppleTalk. La implementación soporta la modalidad de direccionador completo y la modalidad de semidireccionador. Para obtener información adicional, consulte la sección “AppleTalk sobre PPP” en la publicación *Consulta de configuración y supervisión de protocolos Volumen 2*.

Banyan VINES Control Protocol

RFC 1763 describe el BVCP. La implementación que IBM hace de BVCP no soporta ninguna opción.

Bridging Control Protocol

BCP se especifica en RFC 1638. La implementación que IBM hace de BCP soporta la opción de identificación de línea IEEE 802.5 y la opción de compresión de tinygramas.

NetBIOS Control Protocol (NBCP) es un NCP propietario desarrollado por Shiva Corporation y que utiliza IBM Dial In Access to LAN Client para OS/2, DOS y Windows para marcación de entrada de un solo usuario. NBCP se utiliza para transportar el tráfico de puente de NetBIOS y LLC/802.2 desde estos clientes,

Utilización de PPP

marcados en un 2216 Servidor DIAL, a una LAN conectada. La implementación que IBM hace de NBSP soporta las opciones Dirección MAC y Proyección de nombres de NetBIOS.

NetBIOS Frame Control Protocol (NBFCP) se especifica en RFC 2097. NBFCP lo utilizan clientes Microsoft Windows[®] 95 y Windows NT[®] Dial-Up Networking para la marcación de entrada de un solo usuario. NBFCP se utiliza para transportar el tráfico de puente de NetBIOS desde estos clientes, marcados en un 2216 Servidor DIAL, a una LAN conectada. La implementación que IBM hace de NBFCP soporta las opciones Proyección de nombres, Información de igual y Dirección MAC necesaria IEEE.

Callback Control Protocol

Nota: CBCP sólo está disponible en interfaces que tienen configurados circuitos de marcación de entrada IBM DIAL.

Callback Control Protocol (CBCP) lo utilizan los clientes Microsoft Dial-Up Networking para negociar la llamada de retorno. El 2216 soporta la llamada de retorno para un número de un solo usuario especificado (llamada de retorno voluntaria) y la llamada de retorno para un número de administrador especificado (llamada de retorno necesaria). La opción CBCP de llamada a una lista de números no está soportada.

Los usuarios PPP que desean utilizar la llamada de retorno CBCP deben tener alguna forma de autenticación (como PAP, CHAP, SPAP o MS-CHAP). No hay ningún parámetro de configuración para CBCP. (El cliente determina cuándo se utiliza.) Consulte la sección "Configuración de llamada de retorno PPP" en la página 631 para obtener información acerca de la configuración de usuarios PPP para la llamada de retorno.

DECnet IV Control Protocol

DNCP se especifica en RFC 1762. La implementación que IBM hace no soporta ninguna opción DNCP.

IP Control Protocol

IPCP se especifica en RFC 1332. La implementación que IBM hace soporta las opciones siguientes:

- Compresión de cabecera IP Van Jacobsen, tal como se describe en RFC 1144.
- Petición de una dirección IP

Puede pedirse una dirección IP para esta interfaz. Si está habilitada la Dirección dinámica en la configuración IP para esta interfaz, el igual suministrará la dirección cada vez que se establezca la conexión.

- Dirección IP

El direccionador puede enviar su dirección IP, así como aceptar una dirección IP de un igual, o suministrar una dirección IP a un igual, si se pide. Si el direccionador está configurado para "Enviar nuestra dirección" en una interfaz en particular y la interfaz tiene una dirección IP numerada válida, IPCP envía la dirección en su Petición de configuración inicial como la opción 3 (dirección IP). IPCP también envía su dirección si el igual envía un NAK de configuración con 0.0.0.0 para la opción 3 (dirección IP), si está configurada una dirección numerada válida para esa interfaz PPP. IPCP no enviará ninguna dirección no numerada a su igual.

Un igual puede especificar su dirección (a la que se hace referencia como "Especificada por el cliente"), o pedir una dirección al direccionador enviando 0.0.0.0 para la Opción 3 en su Petición de configuración inicial. El direccionador puede obtener esta dirección del perfil de usuario autenticado o de la interfaz en sí. La dirección del perfil de usuario tiene prioridad sobre la dirección de la interfaz. Si no desea ofrecer ninguna dirección del perfil de usuario, simplemente deje la dirección 0.0.0.0 para este usuario en el perfil y el direccionador ofrecerá la dirección remota configurada para esta interfaz. Si no hay ninguna dirección remota configurada para la interfaz o el perfil de usuario, y el igual continúa pidiendo una dirección, IPCP fallará.

El direccionador añade automáticamente una ruta estática direccionada a la interfaz PPP para la dirección que se negocia satisfactoriamente, permitiendo direccionar los datos adecuadamente al cliente de marcación de entrada. Cuando finaliza la conexión IPCP por cualquier razón, se elimina subsiguientemente esta ruta estática. Por omisión, la máscara de red para esta ruta es 255.255.255.255 (ruta de sistema principal); sin embargo, si se especifica una máscara de red en el perfil del usuario autenticado (consulte la sección "Configuración de la autenticación PPP" en la página 630) puede utilizarse otra máscara de red que no sea esta para permitir el direccionamiento a más de un sistema principal a través del enlace PPP (también se puede utilizar RIP u otros protocolos de direccionamiento para descubrir rutas si se desea).

- Compresión de cabecera IP, tal como se describe en RFC 2507, RFC 2508 y RFC 2509.

IPv6 Control Protocol

IPv6 Control Protocol se especifica en RFC 2023. En la implementación que IBM hace de IPv6CP, el direccionador puede enviar su dirección IP, así como aceptar una dirección IP de un igual o suministrar una dirección IP a un igual, si se pide. Si el direccionador está configurado para "Enviar nuestra dirección" en una interfaz en particular y esta interfaz tiene una dirección IP numerada y válida, IPv6CP envía la dirección en su Petición de configuración inicial como la opción 3 (Dirección IP). IPv6CP también envía su dirección si un igual envía un NAK de configuración con ::/0 para la opción 3 (dirección IP), si está configurada una dirección numerada y válida para esta interfaz PPP. IPv6CP no enviará ninguna dirección no numerada a su igual.

Un igual puede especificar su dirección (a la que se hace referencia como "Especificada por el cliente"), o pedir una dirección del direccionador enviando ::/0 para la Opción 3 en su Petición de configuración inicial. El direccionador obtiene esta dirección de la interfaz. Si no hay ninguna dirección remota configurada para la interfaz y el igual continúa pidiendo una dirección, IPv6CP fallará.

El direccionador añade automáticamente una ruta estática direccionada a la interfaz PPP para la dirección que se negocia satisfactoriamente, permitiendo direccionar los datos adecuadamente al cliente de marcación de entrada. Cuando finaliza la conexión IPv6CP por cualquier razón, se elimina subsiguientemente esta ruta estática. Por omisión, la longitud del prefijo para esta ruta es de 128 (ruta de sistema principal).

IPX Control Protocol

IPXCP se especifica en RFC 1552. La implementación que IBM hace no soporta ninguna opción IPXCP.

Utilización de PPP

OSI Control Protocol

OSICP se especifica en RFC 1377. La implementación que IBM hace de OSICP no soporta ninguna opción.

APPN HPR Control Protocol

El protocolo de control Advanced Peer-to-Peer Networking® (APPN) High Performance Routing (HPR) se especifica en RFC 2043. No se negocia ninguna opción para este protocolo de control.

APPN ISR Control Protocol

El protocolo de control Advanced Peer-to-Peer Networking (APPN) Intermediate Session Routing (ISR) se especifica en RFC 2043. No se negocia ninguna opción para este protocolo de control.

Consulte la sección “Utilización y configuración de encriptación de datos” de la publicación *Utilización y configuración de las características* para obtener información acerca de la configuración del cifrado para una interfaz PPP.

Utilización y configuración de conexiones virtuales

Las Conexiones virtuales (VC) son circuitos de marcación de entrada DIAL que pueden suspenderse cuando están inactivos durante un período de tiempo predeterminado. La posibilidad de suspender las conexiones puede ayudar a controlar los costes de la red ahorrando el pago de línea para clientes de marcación de entrada DIAL que no están activos; en lugar de mantener activas las conexiones, el sistema guarda información de la sesión y cierra la llamada. Cuando el mismo cliente de marcación de entrada DIAL se vuelve a conectar al servidor, se restaura la información de la sesión y la conexión se reanuda como si no hubiese habido ninguna interrupción. Consulte la sección “Configuración de un VC” en la página 637 para obtener más información.

Puede configurar los servidores DIAL para que finalicen los VC que se han suspendido durante un período de tiempo especificado. También puede finalizar manualmente un VC en cualquier momento. Consulte el mandato **set** DIAL y la sección “DIAL Global Monitoring Commands” de la publicación *Utilización y configuración de las características* para ver los mandatos relacionados.

Consideraciones acerca de VC

Recuerde lo siguiente al configurar los VC:

- Sólo puede utilizar la lista local AAA o la autenticación RADIUS cuando utilice los VC.
- Un VC no soportará IPX. Cuando configure un usuario para que utilice los VC, se inhabilitará el soporte de IPX para ese usuario.
- La configuración del cliente controla la suspensión y la reanudación de un VC. El servidor DIAL no puede controlar este aspecto de la conexión.
- Puede establecerse un VC a través de un paquete MP.
- Los VC no pueden ejecutarse a través de L2TP.
- Los VC suspendidos no se pueden visualizar con las herramientas actuales de gestión de la red.

- No asigne una dirección IP a usuarios remotos por interfaz. Debido a que otro cliente podría utilizar una interfaz con la que un cliente establece un VC, cuando el VC intenta volverse a conectar con el servidor, la conexión fallará porque la dirección IP está en uso.
- Un cliente de marcación de entrada debe utilizar SPAP para la autenticación.

Configuración de un VC

Configure los VC cuando añada un cliente DIAL en el indicador `Config>`. Cuando configure el usuario, puede utilizar los valores por omisión de marcación de entrada DIAL (consulte el mandato **set** de DIAL en el manual *Utilización y configuración de las características*) para ver el tiempo máximo de suspensión y el tiempo de espera excedido de inactividad, o configure valores específicos para el cliente en particular. El ejemplo siguiente muestra la configuración mínima de un VC para un cliente de marcación de entrada DIAL “jose.”

```

)>Config>
Config> add ppp
Enter user name: []? jose
Password:
Enter password again:
Is this a 'DIALs' user? (Yes, No): [Yes]
Type of route? (hostroute, netroute): [hostroute]
IP address: [0.0.0.0]?
Enter hostname for dynamic DNS: []?
Allow Virtual Connections? (Yes, No): [No] Yes
Use Box Default inactivity timeout value and maximum suspended time? (Yes, No): [Yes] No
User-based Max Suspend Time (hours)
0-48 0-unlimited: [12]? 10
User-based Inactivity Timeout (seconds)
10-1024: [30]? 60
Give 'jose' default time allotted? (Yes, No): [Yes]
Enable callback for 'jose'? (Yes, No): [No]
Will 'jose' be able to dial-out? (Yes, No): [No]

PPP user name: jose
User IP address: Interface Default
Netroute Mask: 255.255.255.255
Hostname:
Time allotted: Box Default
Callback type: Not Enabled
Dial-out: Not Enabled

Is information correct? (Yes, No, Quit): [Yes]
User 'jose' has been added
Config>

```

Para visualizar los valores por omisión a nivel de máquina para las conexiones virtuales máximas, el período de tiempo de espera excedido de desocupado y el tiempo de suspensión global máximo por omisión, utilice el mandato `DIALs config>list vc-parameters` en la característica DIAL. Para visualizar cualquier parámetro junto con el tiempo máximo de suspensión y el tiempo de espera excedido de inactividad para todas las conexiones virtuales, utilice el mandato **list all** en la característica DIAL. Consulte la sección “DIAL Global Monitoring Commands” de la publicación *Utilización y configuración de las características*.

Capítulo 44. Configuración y supervisión de interfaces Point-to-Point Protocol

Este capítulo describe los mandatos de configuración y operativos de la interfaz Point-to-Point Protocol en el dispositivo. Las secciones de este capítulo son:

- “Acceso al proceso de configuración de interfaces”
- “Mandatos de configuración Point-to-Point” en la página 640
- “Acceso al proceso de supervisión de interfaces” en la página 661
- “Mandatos de supervisión Point-to-Point” en la página 662
- “Interfaces Point-to-Point Protocol y el mandato interface de GWCON” en la página 686
- “Soporte para la reconfiguración dinámica de Point-to-Point Protocol” en la página 689

Acceso al proceso de configuración de interfaces

Utilice el procedimiento siguiente para acceder al proceso de configuración del direccionador. Este proceso proporciona acceso al proceso de *configuración* de una interfaz específica.

1. En el indicador OPCON (*), entre el mandato **status** para buscar el PID para CONFIG. (Consulte la página 9 para ver una salida de ejemplo del mandato **status**.)
2. En el indicador OPCON, entre el mandato **talk** de OPCON y el PID para CONFIG. (Para ver los detalles de este mandato, consulte la sección “¿Qué es el proceso OPCON?” en la página 33.) Por ejemplo:

```
* talk 6
```

Después de entrar el mandato talk 6, se visualiza el indicador CONFIG (Config>) en la consola. Si no aparece el indicador cuando entre en **CONFIG** por primera vez, pulse **Intro** de nuevo.

3. En el indicador CONFIG, entre el mandato **list devices** para visualizar los números de las interfaces de red para las que el direccionador está configurado actualmente.
4. Anote los números de interfaz.
5. Entre el mandato CONFIG **network** y el número de la interfaz que desea configurar. Por ejemplo:

```
Config> network 1
```

Ahora, se visualiza el indicador de configuración adecuado (por ejemplo, TKR Config> para red en anillo) en la consola.

Nota: El usuario no puede configurar todas las interfaces de red. Para las interfaces que no se pueden configurar, se recibe el mensaje:

```
That network is not configurable
```

Acceso al indicador de configuración de interfaz PPP

Para visualizar el indicador PPP config>:

1. Entre **list devices** en el indicador Config> para visualizar una lista de interfaces.
2. Si no lo ha hecho todavía, establezca el protocolo de enlace de datos de una de las interfaces serie en PPP entrando **set data-link ppp** en el indicador Config>. Por ejemplo:

Configuración de interfaces PPP (Talk 6)

```
Config> set data-link ppp  
Interface Number [0]? 2
```

- Entre **network** seguido del número de la interfaz PPP. Por ejemplo:

```
Config> network 2  
PPP config>
```

Mandatos de configuración Point-to-Point

La Tabla 78 resume los mandatos de configuración PPP y el resto de esta sección explica estos mandatos. Entre los mandatos en el indicador PPP config>.

Tabla 78. Resumen de los mandatos de configuración Point-to-Point

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página 10.
Disable	Inhabilita la compresión de datos (CCP), el manejo de línea DTR, CHAP, PAP, ECP. También inhabilita la autenticación SPAP en las imágenes de Características de acceso a LAN remota.
Enable	Habilita la compresión de datos (CCP), el manejo de línea DTR, CHAP, PAP, ECP. También habilita la autenticación SPAP en imágenes de Características de acceso a LAN remota.
List	Lista toda la información relacionada con los protocolos de interfaces de punto a punto, los parámetros y las opciones.
Set	Establece los parámetros de línea física (HDLC), los parámetros de LCP, los parámetros genéricos de NCP y diversas opciones específicas de NCP.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página 11.

Disable

Inhabilita la compresión de datos, los protocolos de autenticación, los paquetes de mantenimiento PPP, Multilink PPP y la característica Lower DTR.

Sintaxis:

```
disable          ccp  
                  chap  
                  enp  
                  lower-dtr  
                  mp  
                  mppe  
                  mschap  
                  pap  
                  ppp-echo
```

ccp Inhabilita la utilización de la compresión de datos en la interfaz. Consulte la sección “Configuración y supervisión de compresión de datos” de la publicación *Utilización y configuración de las características* para obtener más información.

chap Inhabilita la utilización de Challenge-Handshake Authentication Protocol.

Configuración de interfaces PPP (Talk 6)

Consulte la sección “Challenge-Handshake Authentication Protocol (CHAP)” en la página 629 para obtener más información.

ecp Esto permite que el direccionador no fuerce la utilización del cifrado ECP en esta interfaz. La interfaz seguirá aceptando y ejecutando el Encryption Control Protocol (ECP) si el similar utiliza el ECP.

Nota: El soporte del cifrado es opcional y debe añadirse a la carga del software utilizando el mandato **load add**. Consulte el mandato **load** del proceso de configuración en el manual *Nways Multiprotocol Access Services Guía del usuario de software*.

El uso del cifrado múltiple (utilizar el cifrado en la Capa de seguridad de IP y en la Capa de enlace de datos de PPP o Frame Relay) en el direccionador está restringido por la legislación de exportación del Gobierno de los Estados Unidos. Sólo está soportado en cargas de software bajo un estricto control de la exportación (cargas de software que dan soporte a RC4 con claves de 128 bits y DES triple).

lower-dtr

Determina la forma en que se maneja la señal de terminal de datos preparado (DTR) para las interfaces de línea serie alquiladas que están inhabilitadas. Si se establece este parámetro en “inhabilitado” (valor por omisión) y la interfaz está inhabilitada, no se desactiva la señal DTR.

mp Inhabilita Multilink Protocol (MP) en esta interfaz. Consulte el “Capítulo 45. Utilización de Multilink PPP Protocol” en la página 691 para obtener más información.

Ejemplo:

```
disable mp
Disabled as a MP link
```

mppe Inhabilita Microsoft Point-to-Point Encryption (MPPE) en esta interfaz.

Nota: El soporte de cifrado es opcional y debe añadirse a la carga de software utilizando el mandato **load add**. Consulte la sección “Load” en la página 101.

mschap

Inhabilita la autenticación MS-CHAP en esta interfaz. La inhabilitación de MS-CHAP tiene dos efectos en MPPE, dependiendo de si MPPE está configurado como obligatorio u opcional. Si MPPE es obligatorio, la inhabilitación de MS-CHAP desactiva el enlace. Si MPPE es opcional, la inhabilitación de MS-CHAP inhabilita MPPE en el enlace. Consulte la sección “Autenticación Microsoft CHAP de PPP (MS-CHAP)” en la página 629 para obtener más información.

pap Inhabilita la utilización de Password Authentication Protocol. Consulte la sección “Password Authentication Protocol (PAP)” en la página 629 para obtener más información.

ppp-echo

Inhabilita el envío de paquetes de mantenimiento PPP.

spap Inhabilita la utilización de Shiva Password Authentication Protocol (SPAP).

Nota: SPAP sólo está disponible en interfaces que tienen configurados circuitos de marcación de entrada IBM DIAL.

Configuración de interfaces PPP (Talk 6)

Enable

Habilita la compresión de datos, el cifrado, los protocolos de autenticación, lower-DTR, paquetes de mantenimiento PPP y el protocolo Multilink PPP en esta interfaz PPP. Si hay varios protocolos de autenticación habilitados, el dispositivo intenta utilizarlos con el siguiente orden de prioridad.:

1. MS-CHAP
2. CHAP
3. PAP

Sintaxis:

```
enable                ccp  
                        chap  
                        ecp  
                        lower-dtr  
                        mp  
                        mppe  
                        mschap  
                        pap  
                        ppp-echo
```

ccp Habilita la utilización de la compresión de datos en la interfaz.

Nota: No se recomienda habilitar la compresión de datos para una interfaz de datos de un adaptador HSSI.

chap Habilita la utilización de Challenge-Handshake Authentication Protocol. Se le solicita un intervalo de cuestión de la identidad. Especifique 0 si no desea cuestionar la identidad periódicamente después de completar la fase de autenticación inicial. Consulte la sección “Challenge-Handshake Authentication Protocol (CHAP)” en la página 629 para obtener más información.

Ejemplo:

```
enable chap  
Rechallenge Interval in seconds (0=NONE) [0] 10  
CHAP enabled
```

ecp Habilita la utilización del cifrado de datos en esta interfaz mediante la negociación de Encryption Control Protocol (ECP). Una vez hecho esto, todos los usuarios PPP con el cifrado habilitado y con una clave de cifrado válida deben utilizar ECP para conectarse a este puerto a menos que MS-CHAP sea el protocolo de autenticación activo para el enlace. Si el protocolo de autenticación es MS-CHAP, no se puede utilizar ECP; el cifrado debe efectuarse utilizando MPPE. Los usuarios PPP sin el cifrado habilitado seguirán pudiendo conectarse a esta interfaz.

Cuando habilita ECP, se le solicita que entre la clave de cifrado ECP para el direccionador local. También debe proporcionar la clave de cifrado para el usuario remoto cuando utilice el mandato **add ppp-user** de talk 6 en el indicador `Config>` para configurar el usuario remoto. MPPE no necesita que configure ninguna clave de cifrado en el usuario local o remoto.

Configuración de interfaces PPP (Talk 6)

Nota: El soporte de cifrado es opcional y debe añadirse a la carga de software utilizando el mandato **load add**. Consulte la sección “Load” en la página 101.

lower-dtr

Determina la forma en que se maneja la señal de terminal de datos preparado (DTR) para las interfaces de línea serie alquiladas que están inhabilitadas. Si se establece este parámetro en “inhabilitado” (valor por omisión) y la interfaz está inhabilitada, no se desactiva la señal DTR.

Si Lower DTR se establece en “habilitada”, la señal DTR se desactivará cuando se inhabilite la interfaz. Este comportamiento puede ser aconsejable en situaciones en las que se ha configurado la interfaz como un enlace alternativo para el Redireccionamiento de WAN y la interfaz está conectada a un módem de marcación de salida que mantiene su conexión de marcación basándose en el estado de la señal DTR.

Cuando se inhabilita la interfaz, la señal DTR se desactiva y el módem mantiene desactivada la conexión de marcación. Cuando la interfaz está habilitada, debido a un escenario de seguridad de Redireccionamiento de WAN, se emite el DTR y el módem marca un número almacenado para el sitio de seguridad. Cuando se restaura la interfaz primaria, se inhabilita la interfaz alternativa, el DTR se desactiva y el módem deja en suspenso la conexión de marcación.

Se dan soporte a los tipos de cable siguientes:

- RS-232
- V.35
- V.36

Nota: El mandato **enable lower-dtr** no está soportado en interfaces de circuito de marcación PPP.

mp Habilita Multilink Protocol (MP) en esta interfaz. Consulte la sección “Capítulo 45. Utilización de Multilink PPP Protocol” en la página 691 para obtener más información.

Ejemplo:

```
enable mp
Enabled as a MP link
Is this link a dedicated MP link? [no] yes
MP interface for this MP link? [0] 3
```

mppe *[mandatory/optional] [stateless/stateful]*

Habilita Microsoft Point-to-Point Encryption (MPPE). Si MS-CHAP no está habilitado en la interfaz, no puede habilitarse MPPE en esta interfaz. Consulte la sección Microsoft Point-to-Point Encryption (MPPE) del capítulo “Utilización y configuración de protocolos de encriptación” en la publicación *Utilización y configuración de las características* para obtener más información.

mandatory

El cliente y el servidor deben negociar MPPE o se desactivará el enlace.

optional

El cliente intentará negociar MPPE, pero si falla la negociación, el enlace PPP seguirá activo.

stateless

Las claves de sesión se volverán a generar después de transmitir

Configuración de interfaces PPP (Talk 6)

cada paquete. Esta función no está soportada actualmente por los clientes Microsoft Dial-Up Networking (DUN).

stateful

Las claves de sesión se volverán a generar después de transmitir 256 paquetes.

Nota: El soporte de cifrado es opcional y debe añadirse a la carga de software utilizando el mandato **load add**. Consulte la sección “Load” en la página 101 para obtener más información.

mschap

Habilita la autenticación MS-CHAP. Cuando se habilita MS-CHAP, se solicita al usuario que proporcione un intervalo de cuestión de la identidad al autenticador. Este valor en segundos define el período de tiempo que pasará antes de que el autenticador envíe otra cuestión de la identidad al receptor de la petición de autenticación para volver a confirmar la autenticación. El valor 0 indica que no se enviarán más cuestiones de la identidad después de la autenticación inicial.

Utilice el mandato **set name** para configurar el nombre del 2216 si el direccionador similar está configurado para autenticar el nombre local del 2216.

Observe que MS-CHAP no puede habilitarse si se ha configurado un servidor de autenticación externo, tal como se describe en el capítulo “Utilización de autenticación local o remota” de la publicación *Utilización y configuración de las características*. Consulte la sección “Autenticación Microsoft CHAP de PPP (MS-CHAP)” en la página 629 para obtener más información.

pap Habilita la utilización de Password Authentication Protocol. Consulte la sección “Password Authentication Protocol (PAP)” en la página 629 para obtener más información.

ppp-echo

Habilita el envío de paquetes de mantenimiento PPP, que se utilizan para validar la conexión.

List

Utilice el mandato **list** para visualizar información relacionada con la interfaz PPP y sus parámetros y opciones de protocolo.

Sintaxis:

<u>list</u>	<u>all</u>
	<u>bcp</u>
	<u>ccp</u>
	<u>ecp</u>
	<u>hdlc</u>
	<u>ipcp</u>
	<u>ipv6cp</u>
	<u>lcp</u>
	<u>ncp</u>

Configuración de interfaces PPP (Talk 6)

all Lista todas las opciones y parámetros relacionados con la interfaz PPP.

El mandato **list all** visualiza la salida de *todos* los parámetros **list...** individuales descritos más abajo.

bcp Lista las opciones del protocolo de control Bridging Network.

Ejemplo:

```
list bcp
BCP Options
-----
Tinygram Compression:DISABLED
```

Tinygram Compression:

Visualiza si la Compresión de tinygramas está habilitada/inhabilitada.

ccp Visualiza las opciones de compresión de datos seleccionadas actualmente si se ha habilitado la compresión de datos. Para obtener información adicional, consulte la sección “Configuración y supervisión de compresión de datos” de la publicación *Utilización y configuración de las características*.

Si están habilitados Microsoft Point-to-Point Encryption (MPPE) y la compresión de datos, el tipo de compresión de datos es MPPC.

ecp Visualiza el estado actual de Encryption Control Protocol.

Ejemplo:

```
list ecp
ECP Options
-----
Data Encryption enabled
Algorithm list: DESE-CBC
DESE (Data Encryption Standard Encryption Protocol)
```

Nota: El soporte de cifrado es opcional y debe añadirse a la carga de software utilizando el mandato **load add**. Consulte la sección “Load” en la página 101.

Data Encryption Enabled/Disabled

Indica si el cifrado de datos está habilitado o inhabilitado en la interfaz.

Algorithm List

Visualiza los algoritmos de cifrado soportados. DES, tal como se describe por RFC 1969, es el único algoritmo de cifrado soportado actualmente.

hdlc Lista los parámetros relacionados con el protocolo High-Level Data Link Control (HDLC). En interfaces de circuitos de marcación PPP, la opción “list hdlc” no está disponible. Para circuitos de marcación, los parámetros de enlace de datos de hardware son una función de la red base en lugar del circuito de marcación PPP. Consulte el “Capítulo 54. Configuración y supervisión de circuitos de marcación” en la página 797 para obtener más información.

Ejemplo:

```
list hdlc
Encoding: NRZ
Idle State: Flag
Clocking: Internal
Cable type: V.35 DCE
Speed (bps): 6400

Transmit Delay Counter: 0
Lower DTR: Disabled
```

Configuración de interfaces PPP (Talk 6)

Encoding:

El esquema de codificación de transmisión HDLC, NRZ (sin retorno a cero) o NRZI (inversión sin retorno a cero).

Idle State:

Patrón de bits, distintivo o marca, transmitido en el enlace de punto a punto cuando la interfaz no transmite datos.

Clocking:

Cronometraje de interfaz, externo o interno.

Cable type:

Especifica el tipo de cable que se utiliza (RS-232, V.35 o V.36).

Speed (bps):

La velocidad física de datos de la interfaz. Cuando el cronometraje es interno, es la velocidad de datos generada por el reloj interno.

Transmit Delay Counter:

Número de distintivos enviados entre tramas.

Lower DTR:

Habilitado o inhabilitado. Si Lower DTR está habilitado, el direccionador desactiva la señal DTR cuando ya no es necesario un enlace alternativo de Redireccionamiento de WAN. La desactivación de la señal DTR hace que el módem termine la conexión de línea alquilada para el enlace alternativo.

Notas:

1. El mandato **list hdlc** no está soportado en interfaces de circuitos de marcación PPP.
2. Este mandato sólo visualiza el estado de Lower DTR si Lower DTR está soportado para el tipo de cable configurado.
3. Este mandato para una interfaz PPP de un adaptador HSSI visualiza el subconjunto de parámetros HDLC listados anteriormente.

ipcp Lista las opciones del protocolo de control Internet Protocol.

Ejemplo: Cuando se configura la Compresión de cabeceras RTP:

```
list ipcp
IPCP Options
-----
IPCP Compression: RFC2508 TCP/UDP/RTP Format
TCP Compression Slots: 16
Non-TCP Compression Slots: 16
Max Period: 256
Max Time: 5
Max Header: 168
Start Port: 5004
End Port: 5515
Request an IP Address: No
Send Our IP Address: No
Remote IP Address to Offer if Requested: None
PPP 0 Config>
```

Ejemplo: Cuando se configura la Compresión de cabeceras VJ:

```
IPCP Options
-----
IPCP Compression: RFC1144 Van Jacobson Compression Slots: 16
Request an IP Address: No
Send Our IP Address: No
Remote IP Address to Offer if Requested: None
PPP 0 Config>
```

Configuración de interfaces PPP (Talk 6)

IPCP compression

Indica si el manejador PPP va a aceptar cabeceras IP comprimidas.

VJ or RTP Header Compression

PPP soporta la compresión de cabeceras TCP/IP Van Jacobson (RFC 1144), así como la compresión de cabeceras IP/UDP/RTP (RFC2508). Habilite una de ellas cuando el enlace de punto a punto esté ejecutando a una velocidad en baudios baja. El valor VJ indica que se va a utilizar RFC 1144. El valor RTP indica que se va a utilizar RFC 2508.

Request an IP Address

Indica si IPCP está configurado para recuperar la dirección IP local para esta interfaz PPP desde el extremo remoto del enlace en la "Petición de configuración" inicial.

Send Our IP Address

Indica si IPCP está configurado para enviar la dirección IP local para esta interfaz PPP al extremo remoto del enlace en la "Petición de configuración" inicial. Algunas implementaciones de PPP necesitan esta información.

ipv6cp

Lista las opciones del protocolo de control de Internet Protocol versión 6.

Ejemplo:

```
list ipv6cp
IPv6CP Options
-----
Send Our IP Address:          Yes
```

Send Our IP Address

Indica si IPv6CP está configurado para enviar la dirección IP local para esta interfaz PPP al extremo remoto del enlace en la "Petición de configuración" inicial. Algunas implementaciones de PPP necesitan esta información.

lcp

Lista los parámetros y opciones para Link Control Protocol.

Ejemplo:

PPP 7 Config>list lcp

```
LCP Parameters
-----
Config Request Tries:      20  Config Nak Tries:      10
Terminate Tries:          10  Retry Timer:           3000

LCP Options
-----
Max Receive Unit:          1522  Magic Number:          Yes
Peer to Local (RX) ACCM:   A0000
Protocol Field Comp(PFC):  No    Addr/Cntl Field Comp(ACFC): No

Authentication Options
-----
Authenticate remote using: none
Identify self as:         ibm
```

Link Control Protocol incluye los protocolos de autenticación utilizados para autenticar el similar remoto. Si el protocolo de autenticación es CHAP o Microsoft PPP CHAP (MS-CHAP), se visualiza el intervalo de cuestión de la identidad.

Ejemplo:

Configuración de interfaces PPP (Talk 6)

PPP 7 Config>list lcp

```
LCP Parameters
-----
Config Request Tries:      20   Config Nak Tries:      10
Terminate Tries:          10   Retry Timer:           3000

LCP Options
-----
Max Receive Unit:          1522   Magic Number:          Yes
Peer to Local (RX) ACCM:   A00000
Protocol Field Comp(PFC):  No    Addr/Cntl Field Comp(ACFC): No

Authentication Options
-----
Authenticate remote using:  MSCHAP or SPAP or CHAP or PAP [Listed in priority order]
CHAP Rechallenge Interval: 0
MSCHAP Rechallenge Interval: 0
Identify self as:          ibm
```

Config Request Tries:

Número de veces que LCP envía paquetes de petición de configuración a una estación similar mientras intenta abrir un enlace PPP.

Config Nak Tries:

Número de veces que LCP envía paquetes de no reconocimiento de configuración (“sin reconocimiento”) a una estación similar mientras intenta abrir un enlace PPP.

Terminate Tries:

Número de veces que LCP envía paquetes de petición de terminación a una estación similar para cerrar un enlace PPP.

Retry Timer:

Número de milisegundos que transcurren antes que continúe la transmisión de paquetes de acuerdo al número de veces establecido por el parámetro “Intentos de configuración”.

Max Receive Unit:

Visualiza el tamaño máximo de campo de información (paquete) manejado por el enlace.

Peer to Local (Rx) ACCM

Visualiza los caracteres para los que el similar debe ejecutar “escape” cuando transmite paquetes al direccionador en líneas asíncronas.

Magic Number:

Indica si está habilitada la opción de detección de bucle de retorno de número mágico.

Protocol Field Comp (PFC):

Indica si la opción PFC está habilitada.

Addr/Cntl Field Comp(ACFC):

Indica si ACFC está habilitada.

Authenticate remote using:

Una lista de protocolos de autenticación habilitados.

Identify Self As:

El nombre establecido con el mandato **set name**.

ncp Lista los parámetros para todos los Network Control Protocols.

Ejemplo:

Configuración de interfaces PPP (Talk 6)

```
list ncp
NCP Parameters
-----
Config Request Tries:      20  Config Nak Tries:      10
Terminate Tries:          10  Retry Timer:           3000
```

Config Request Tries:

Número de veces que NCP envía paquetes de petición de configuración a una estación similar mientras intenta abrir un enlace PPP.

Terminate Tries:

En espera de un reconocimiento de terminación, el número de veces que NCP envía una Petición de terminación antes de cerrar un enlace PPP.

Config Nak Tries:

Número de veces que NCP envía paquetes de no reconocimiento de configuración a una estación similar mientras intenta abrir un enlace PPP.

Retry Timer:

Número de milisegundos que transcurren antes de exceder el tiempo de espera de la transmisión de NCP de paquetes de petición de configuración (para abrir el enlace) y paquetes de petición de terminación (para cerrar el enlace).

LLC

Utilice el mandato **LLC** para acceder al entorno de configuración LLC (sólo disponible si APPN se incluye en la carga de software). Consulte la sección “Mandatos de configuración LLC” en la página 251 para ver una explicación de cada uno de estos mandatos.

Sintaxis:

llc

Set

Utilice el mandato **set** para establecer los parámetros HDLC, las opciones y los parámetros LCP, las opciones IPCP, las opciones BCP y los parámetros NCP. Los “parámetros” están relacionados con operaciones internas como, por ejemplo, cuentas de reintentos. Las “opciones” son elementos que se negocian con el otro extremo.

Notas:

1. Los valores que siguen inmediatamente a los indicadores de la opción del mandato reflejan el valor actual de esa opción. No siempre son los valores por omisión ilustrados en este capítulo.
2. Los mandatos **set hdlc** no están soportados en las interfaces de circuitos de marcación PPP.

Sintaxis:

```
set                                bcp
                                     ccp options
                                     ccp algorithms
                                     hdlc...
                                     ipcp
```

Configuración de interfaces PPP (Talk 6)

ipv6cp
lcp...
name...
ncp...

bcp Establece los parámetros de Bridging Control Protocol (BCP).

Ejemplo:

```
set bcp  
TINYGRAM COMPRESSION [no]:
```

Tinygram Compression

Especifica si se utiliza la Compresión de tinygramas o no. Esta opción es útil para los protocolos que son propensos a tener problemas cuando se establecen puentes a través de líneas de baja velocidad (64 kbps y menos). Estos protocolos añaden ceros entre los datos y la suma de comprobación de la trama para rellenar la Unidad de datos de protocolo (PDU) hasta el tamaño mínimo. La compresión de tinygramas elimina los ceros y conserva la suma de comprobación de la trama en el extremo de transmisión. En el extremo de recepción, restaura el paquete a la longitud mínima.

ccp options

Le solicita las opciones configurables para los algoritmos de compresión. Algunas de las opciones pueden modificarse después mediante negociaciones de PPP con el direccionador similar del enlace WAN. Consulte la sección “Configuración y supervisión de compresión de datos” en la publicación *Utilización y configuración de las características* para obtener más información.

Ejemplo:

```
set ccp options  
STAC: check mode (0=none, 1=LCB, 2=CRC, 3=Seq, 4=Ext) [3]?  
STAC: # histories [1]?
```

STAC: check mode (0=none, 1=LCB, 2=CRC, 3=Seq, 4=Ext)

Normalmente, los datagramas comprimidos con STAC incluyen un valor de comprobación utilizado por los dos extremos del enlace para reconocer cuándo se ha perdido o dañado un paquete comprimido y es necesaria alguna acción para volver a sincronizar los históricos del emisor y del receptor.

Nota: Si no se puede detectar un paquete anómalo puede provocar la descompresión incorrecta de todos los datos subsiguientes.

Esta opción establece el formato exacto del valor de comprobación utilizado. Elija uno de los siguientes:

- 0** Ninguno: No se utiliza ningún valor de comprobación. Sin un valor de comprobación, no hay manera de determinar si un paquete se ha perdido, está fuera de secuencia o se ha dañado. No utilice esta modalidad a menos que el enlace de datos básico proporcione una entrega de paquetes fiable y secuenciada.
- 1** LCB: Se utiliza un “Byte de control longitudinal”. Se trata de una simple suma de comprobación OR exclusiva de 8 bits.

Configuración de interfaces PPP (Talk 6)

Se desaconseja encarecidamente su utilización porque el receptor no puede detectar un paquete perdido o fuera de secuencia y la suma de comprobación de la trama PPP es una prueba más fiable de la integridad del paquete.

- 2 CRC: Se utiliza una suma de comprobación de redundancia cíclica de 16 bits. Aunque se trate de una prueba mejor de la integridad de un paquete que LCB, se sigue desaconsejando su utilización porque el receptor tampoco puede utilizarla para detectar si los paquetes se han perdido o están fuera de secuencia y, por otro lado, es muy redundante con la suma de comprobación de la trama.
- 3 SEQ: Se utiliza un número de secuencia de 8 bits (valor por omisión). Es el método preferido de funcionamiento. Si el número de históricos no es 0, se desaconseja encarecidamente la utilización de cualquier otra modalidad aunque puede que sea necesaria otra modalidad para la interoperatividad con determinados direccionadores que no se ajustan a RFC.
- 4 EXT: Una modalidad ampliada que es similar a la modalidad de número de secuencia en la que cada paquete incluye un número de secuencia pero el formato de trama comprimida se altera más radicalmente. En la modalidad ampliada, la resincronización con un similar se realiza de forma diferente que en las otras modalidades; la señalización entre los dos nodos se basa en distintivos pasados en las cabeceras de los datagramas comprimidos en lugar de paquetes de control CCP diferenciados.

La modalidad ampliada se proporciona para la compatibilidad con ciertas implementaciones que no se ajustan a RFC. Sólo debe utilizarse con clientes que no soportan la modalidad 3.

STAC: # histories

Establece el número de "contextos" o "históricos" de compresión que utiliza el mecanismo de compresión STAC.

Un valor distinto de cero significa que el mecanismo de compresión mantiene el número especificado de históricos donde guarda información acerca de datos enviados anteriormente en paquetes. Estos datos del histórico se utilizan para mejorar la eficacia de la compresión.

El receptor mantiene un histórico similar y siempre que el transmisor y el receptor mantengan sus históricos sincronizados, el receptor puede descomprimir correctamente los paquetes que recibe. Si los históricos no están sincronizados, se eliminan los paquetes como datos no utilizables. Normalmente, debe establecer el número de históricos en 1 a menos que la calidad del enlace sea muy pobre.

Un valor de cero significa que se comprimen todos los paquetes enviados sin tener en cuenta ningún paquete enviado con anterioridad y siempre puede ser descomprimido fiablemente por el receptor. Sin embargo, debido a que el compresor no puede

Configuración de interfaces PPP (Talk 6)

explotar ninguna información derivada del examen de paquetes anteriores, normalmente la eficacia de la compresión no es tan buena.

Algunas implementaciones soportan más de un histórico, subdividiendo la corriente de datos en corrientes separadas que se comprimen independientemente. El direccionador no soporta la utilización de más de un histórico en un enlace PPP.

ccp algorithms *lista-de-algoritmos*

Especifica una lista exacta de los algoritmos de compresión que se han de utilizar. El orden de prioridad depende del orden de entrada en la lista. Cuando MPPE está activado en el enlace, se pasa por alto el orden de los algoritmos CCP y sólo se utiliza Microsoft Point-to-Point Compression (MPPC).

Cuando el enlace negocia la compresión con otro nodo, ofrece toda la lista de protocolos al nodo similar por orden de prioridad. El nodo similar debe seleccionar el primer protocolo que pueda utilizar de la lista de preferencias. La habilitación de múltiples protocolos permite que el similar imponga el algoritmo de compresión que se utilizará en el enlace. Si necesita evitar un algoritmo, no especifique el algoritmo en la lista.

La especificación de **none** inhabilita la utilización de cualquier protocolo que inhabilite efectivamente la compresión. Los algoritmos de compresión válidos son:

STAC-LZS

El algoritmo STAC-LZS tal como se describe en RFC 1974

MPPC El algoritmo Microsoft Point-to-Point Compression tal como se describe en RFC 2118.

Ejemplo:

```
set ccp algorithms
PPP 6 Config>set ccp alg
Enter a prioritized list of compression algorithms (first is preferred),
all on one single line.
Choices (can be abbreviated) are:
STAC-LZS MPPC
Compressor list [STAC-LZS]? stac mppc
```

hdlc cable *tipo de cable*

Establezca el tipo de cable HDLC (que se conecta a la interfaz) en uno de los tipos siguientes:

- RS-232 DTE
- RS-232 DCE
- V35 DTE
- V35 DCE
- V36 DTE
- V36 DCE
- X21 DTE
- X21 DCE
- HSSI DTE
- HSSI DCE

La Tabla 79 en la página 653 lista los tipos de cables que puede configurar en los diversos adaptadores.

Configuración de interfaces PPP (Talk 6)

Tabla 79. Tipos de cables para interfaces 2216

Tipo de adaptador	Tipo de cable
EIA 232 de 8 puertos	RS-232 DTE y RS-232 DCE
V.35/V36 de 6 puertos	V.35 DCE, V.35 DTE, V.36 DCE o V.36 DTE
X.21 de 8 puertos	X.21 DCE y X.21 DTE
HSSI de 1 puerto	HSSI DCE y HSSI DTE*

Nota: Cuando se utiliza el cable HSSI DCE, el otro dispositivo también debe estar configurado para utilizar un cable HSSI DCE.

Ejemplo: `set hdlc cable rs-232 dce`

Se utiliza un cable DTE al conectar el direccionador a algún tipo de dispositivo DCE (por ejemplo, un módem o una DSU/CSU).

Se utiliza un cable DCE cuando el direccionador actúa como DCE y proporciona el cronometraje para la conexión directa.

hdlc clocking *external o internal*

Para conectar con un módem o DSU, configure el cronometraje externo y seleccione el cable DTE adecuado con el mandato **set hdlc cable**. Utilice el mandato **set hdlc speed** para configurar la velocidad de línea.

Para conectar directamente con otro dispositivo DTE, configure el cronometraje interno, seleccione el cable DCE adecuado con el mandato **set hdlc cable** y configure el cronometraje/velocidad de línea con el mandato **set hdlc speed**.

Valor por omisión: external

Ejemplo: `set hdlc clocking internal`

Nota: El tipo de cronometraje no es configurable cuando PPP está configurado en un adaptador HSSI. El tipo de cronometraje se determina por el tipo de cable. El cronometraje interno se utiliza cuando está configurado el tipo de cable HSSI DCE y el cronometraje externo se utiliza cuando está configurado el tipo de cable HSSI DTE.

hdlc encoding *NRZ o NRZI*

Establece el esquema de codificación de transmisión HDLC para una interfaz. La codificación puede establecerse para NRZ (sin retorno a cero) o NRZI (inversión sin retorno a cero). NRZ es el esquema de codificación más ampliamente utilizado mientras que NRZI se utiliza en algunas configuraciones de IBM. El valor por omisión es NRZ.

Nota: La codificación se establece en NRZ para una interfaz PPP de un adaptador HSSI y no es configurable.

Ejemplo: `set hdlc encoding nrz`

hdlc idle *flag o mark*

Establece el estado de desocupado del enlace de datos en distintivo o marca.

La opción de distintivo proporciona distintivos continuos (7E hex) entre tramas.

Configuración de interfaces PPP (Talk 6)

La opción de marca pone la línea en estado de marca (OFF, 1) entre tramas.

Nota: Desocupado se establece en *distintivo* para una interfaz PPP de un adaptador HSSI y no es configurable.

Ejemplo: set hdlc idle flag

hdlc speed *valor*

Para el cronometraje interno, utilice este mandato para especificar la velocidad de las líneas de reloj de transmisión y recepción.

Para el cronometraje externo, este mandato no afecta al funcionamiento de la WAN/línea serie pero establece la velocidad que algunos protocolos, como IPX, utilizan para determinar los parámetros de coste de direccionamiento. Debe establecer la velocidad de manera que coincida con la velocidad real de la línea. Si no está configurada la velocidad, los protocolos suponen una velocidad de 1 000 000 bps.

Valores válidos:

Cronometraje interno: Consulte la Tabla 80

Cronometraje externo: Consulte la Tabla 81

Tabla 80. Velocidades de línea cuando se utiliza el cronometraje interno para interfaces 2216

Tipo de adaptador	Rango de velocidades
EIA 232 de 8 puertos	De 9600 a 64 000 bps
V.35/V.36 de 6 puertos	De 9600 a 460 800 bps, 1 544 000 bps ó 2 048 000 bps
X.21 de 8 puertos	De 9600 a 460 800 bps, 1 544 000 bps ó 2 048 000 bps
HSSI de 1 puerto	22 368 000 bps ó 44 736 000 bps

Tabla 81. Velocidades de línea cuando se utiliza el cronometraje externo para interfaces 2216

Tipo de adaptador	Rango de velocidades
EIA 232 de 8 puertos	De 2400 a 64 000 bps
V.35/V.36 de 6 puertos	De 2400 a 2 048 000 bps
X.21 de 8 puertos	De 2400 a 2 048 000 bps
HSSI de 1 puerto	De 1 544 000 bps a 52 000 000 bps

Ejemplo: set hdlc speed 56 000

hdlc transmit-delay *valor*

Establece el número de distintivos entre tramas. El propósito de este mandato es moderar la velocidad de la línea serie para que sea compatible con los dispositivos serie más antiguos y lentos del otro extremo.

El rango es de 0 a 15. El valor por omisión es 0.

Nota: Si configura un retardo de transmisión que no es cero para una interfaz PPP del adaptador EIA- 232E de 8 puertos, el adaptador V.35/V.36 de 6 puertos o el adaptador X.21 de 8 puertos, debe configurar la velocidad de línea utilizando el mandato **set hdlc speed**.

Ejemplo: set hdlc transmit-delay 15

ipcp Establece todas las opciones de Internet Protocol Control Protocol para este enlace.

Ejemplo: Configuración de la compresión de cabeceras RTP

```
PPP 0 Config>set ipcp
IP COMPRESSION [yes]:
VJ or RTP Header Compression [RTP]:
  Max Period: [256]?
  Max Time: [5]?
  Max Header: [168]?
  RTP Start Port: [5004]?
  RTP End Port: [5515]?
  Number of TCP Slots: [16]?
  Number of Non-TCP Slots: [16]?
Request an IP address [no]:
Send our IP address [no]:
Note: unnumbered interface addresses will not be sent.
Interface remote IP address to offer if requested (0.0.0.0 for none) [0.0.0.0]?
```

Ejemplo: Configuración de la compresión de cabeceras VJ

```
PPP 0 Config>set ipcp
IP COMPRESSION [yes]:
VJ or RTP Header Compression [VJ]:
  Number of TCP Slots: [16]?
Request an IP address [no]:
Send our IP address [no]:
Note: unnumbered interface addresses will not be sent.
Interface remote IP address to offer if requested (0.0.0.0 for none) [0.0.0.0]?
PPP 0 Config>
```

IPCP compression

Indica si el manejador PPP va a aceptar cabeceras IP comprimidas.

El establecimiento de este valor en **yes** habilita la opción de compresión. El establecimiento de este valor en **no** inhabilita la opción. El valor por omisión es **no**.

VJ or RTP Header Compression

PPP soporta la compresión de cabeceras TCP/IP Van Jacobson (RFC 1144), así como la compresión de cabeceras IP/UDP/RTP (RFC2508). Habilite una de ellas cuando el enlace de punto a punto esté ejecutando a una velocidad en baudios baja. El valor VJ indica que se va a utilizar RFC 1144. El valor RTP indica que se va a utilizar RFC 2508.

Las descripciones que siguen dependen de si se ha especificado VJ o RTP. Si es VJ, el único parámetro configurado es Number of TCP Slots.

Max Period

Especifica el número máximo de cabeceras comprimidas que pueden enviarse antes de que deba enviarse una cabecera completa para renovar la información de cabecera almacenada en la ranura.

Valores válidos: De 1 a 65 535

Valor por omisión: 256

Max Time

Especifica el número máximo de segundos que pueden enviarse cabeceras comprimidas antes de que deba enviarse una cabecera completa para renovar la información de cabecera almacenada en la ranura.

Configuración de interfaces PPP (Talk 6)

Valores válidos: De 1 a 255

Valor por omisión: 5

Max Header

Especifica la cabecera mayor (en bytes) que se espera que procese el compresor.

Valores válidos: De 60 a 65 535

Valor por omisión: 168

RTP Start Port

Especifica el inicio del rango completo de puertos UDP utilizados por RTP.

Valores válidos: De 5004 a 65 534

Valor por omisión: 5004

RTP End Port

Especifica el final del rango completo de puertos UDP utilizados por RTP.

Valores válidos: De 5005 a 65 534

Valor por omisión: 5515

Number of TCP Slots

Establece el número de cabeceras TCP/IP que se guardan al comprimir cabeceras TCP/IP.

Valores válidos: De 1 a 16

Valor por omisión: 16

Number of Non-TCP slots

Establece el número de cabeceras UDP/IP y RTP/UDP/IP que se guardan al comprimir cabeceras TCP/IP.

Valores válidos: De 1 a 16

Valor por omisión: 16

Request an IP address

Especifica si la dirección IP local para esta interfaz debe recuperarse desde el extremo remoto del enlace. Debe establecer esta opción en **yes** si el otro extremo de este enlace proporciona la dirección IP. Es una característica típica proporcionada por ISP (Internet Service Providers).

Esta interfaz necesitará tener una configuración IP propia para que se pueda utilizar la dirección pedida. Específicamente, debe habilitarse la Dirección dinámica en esta interfaz.

Nota: La siguiente pregunta, **Send Our IP address**, no se visualizará si **Request an IP address** se establece en **yes**.

Send Our IP address

Especifica si se ha de enviar o no la dirección IP local al extremo remoto del enlace. Debe establecer esta opción en **yes** si el otro extremo del enlace necesita la dirección IP.

Si este valor se establece en **yes**, IPCP enviará la dirección IP de la interfaz PPP, si la interfaz está configurada con una dirección IP numerada, (es decir, la dirección no empieza por 0). Si esta opción

Configuración de interfaces PPP (Talk 6)

se establece en **no** y el similar nos envía un NAK de configuración con 0.0.0.0 para la opción Dirección IP, el 2216 responderá con la dirección de la interfaz PPP si está configurada con una dirección numerada.

ipv6cp

Establece la opción del Protocolo de control IPv6 para el enlace.

Ejemplo:

```
set ipv6cp
Send Our IP address [no]:
```

Send Our IP address

Especifica si se ha de enviar o no la dirección IPv6 local al extremo remoto del enlace. Establezca esta opción en **yes** si el otro extremo del enlace necesita la dirección IPv6.

Si este parámetro se establece en **yes**, IPv6CP enviará la dirección IPv6 de la interfaz PPP, si la interfaz está configurada con una dirección IPv6 numerada, (es decir, la dirección no empieza por 0). Si esta opción se establece en **no** y el similar nos envía un NAK de configuración con ::/0 para la opción de dirección IPv6, el 2216 responderá con la dirección de la interfaz PPP si está configurada con una dirección numerada.

lcp options o parameters

Establece las opciones de Link Control Protocol y los parámetros para el enlace PPP.

Ejemplo:

```
set lcp options
Maximum Receive Unit (bytes) [2048]?
Magic Number [yes]:
Peer-to-Local Async Control Character Map (RX ACCM) [A0000] ?
Protocol Field Compression (PFC) [no]?
Addr/Cntl Field Compression (ACFC) [no]?
```

Maximum receive unit

Establece el tamaño máximo del campo de información que se transfiere en un solo datagrama. El rango es de 576 a 4089 bytes. El valor por omisión es 2048.

Magic number

Especifica si la opción de número mágico está habilitada o no. El número mágico proporciona una manera de detectar enlaces de bucle de retorno en las configuraciones de línea serie. Cuando esta opción está habilitada, el enlace utiliza el reloj del sistema como generador de números aleatorios. Se hace referencia a los números aleatorios que se generan como números mágicos.

Cuando LCP recibe una Petición de configuración con un número mágico (p. ej., la opción de número mágico está habilitada), el número mágico recibido se compara con el número mágico de la última Petición de configuración enviada al similar. Si los dos números mágicos son diferentes, el enlace no se considera de bucle de retorno. Si los dos números son iguales, el manejador PPP intenta desactivar el enlace y activarlo de nuevo para volver a negociar los números mágicos.

El establecimiento de este valor en Yes habilita la opción de número mágico. El establecimiento de este valor en No inhabilita la opción. El valor por omisión es Yes.

Configuración de interfaces PPP (Talk 6)

Async Control Character Map

Indica los caracteres en los que el similar debe ejecutar “escape” al transmitir paquetes al direccionador en líneas asíncronas. Esto permite que ciertos caracteres de control ASCII sensibles como, por ejemplo, XON y XOFF, se transmitan transparentemente a través del enlace.

Especifique una máscara de 32 bits en hexadecimal. Si se establece un bit de la posición 'N' de la máscara, debe ejecutarse escape para el carácter ASCII 'N' correspondiente (LSB es el bit número 0, correspondiente al carácter NUL ASCII).

El valor por omisión para esta opción es '0A0000', que indica que es necesario ejecutar escape en XON y XOFF (control-Q y control-S). Esto sirve para que los módems que utilizan XON/XOFF lleven a cabo el acuerdo del software. Si este no es el problema, se recomienda que cambie ACCM a cero (no se ejecuta escape en ningún carácter).

LCP siempre desea negociar el ACCM, incluso en líneas síncronas y el mandato **list lcp** del proceso de supervisión PPP visualizará el valor negociado. Sin embargo, las líneas síncronas emplean un mecanismo “relleno de bits” en lugar de un mecanismo de “escape”, de modo que normalmente ACCM no tiene significado en líneas síncronas. Puede tener significado si el direccionador está conectado a un módem que realice una conversión de síncrono a asíncrono, en cuyo caso su valor debe reflejar los requisitos del módem conectado en la parte asíncrona.

Addr/Cntl Field Compression (ACFC)

Especifica si el similar puede emplear la compresión de campo de control y de dirección.

Si LCP negocia satisfactoriamente la opción ACFC, significa que pueden omitirse los bytes de los campos de dirección y de control que empiezan cada paquete en los datagramas enviados hacia adelante y hacia atrás en el enlace. Estos bytes son siempre 0xFF 03, de modo que no proporcionan ninguna información real y la habilitación de ACFC significa que los datagramas que se transmiten tendrán dos bytes menos de longitud.

Para ser precisos, si habilita ACFC, indica una posibilidad de la parte de recepción. Si habilita ACFC y LCP lo negocia satisfactoriamente, el otro extremo puede emplear ACFC en los paquetes que transmite al extremo local (la mayoría de opciones PPP funcionan así). El extremo local sólo transmitirá los paquetes *sin* los campos de dirección y de control si el otro extremo también indica su posibilidad de manejar estos paquetes.

La habilitación de ACFC no obliga al otro extremo a enviar paquetes sin los campos de dirección y de control, incluso aunque acepte la opción. La habilitación de ACFC solamente indica al similar que opcionalmente *puede* utilizar ACFC y el direccionador podrá manejar los paquetes de entrada. Si el similar indica que puede manejar ACFC, el direccionador siempre ejecutará ACFC en los paquetes que transmita, sin tener en cuenta si ACFC está habilitado localmente.

Configuración de interfaces PPP (Talk 6)

Los paquetes LCP se envían siempre con los campos de dirección y de control. Esto garantiza que los paquetes LCP reconocerán si hay una pérdida de sincronización de enlace.

Protocol Field Compression (PFC)

Especifica si el similar ha de emplear la compresión del campo de protocolo.

Cuando especifica "yes", si LCP negocia satisfactoriamente la opción PFC, puede omitirse el byte cero inicial del campo "Protocolo" para los valores de protocolo en el rango de '0x0000' a '0x00FF', para ahorrar un byte en los paquetes que se transmiten. Este rango incluye la mayoría de los datagramas de protocolo de capa 3.

Todos los valores de protocolo PPP se asignan de manera que el byte superior del protocolo sea un valor par y el byte inferior sea un valor impar (es una utilización limitada del mecanismo más generalizado descrito por el mecanismo de extensión ISO 3309 para campos de dirección). Por lo tanto, el receptor puede detectar rápidamente cuándo se ha omitido el byte inicial de un valor de protocolo (el primer byte del campo de protocolo es impar en lugar de par), de modo que no existe ambigüedad al interpretar tramas en presencia de PFC.

PFC, como ACFC, tiene la posibilidad de la parte de recepción y se aplica a PFC la descripción anterior de ACFC.

Ejemplo:

```
set lcp parameters
Config tries [20]?
NAK tries [10]?
Terminate tries [10]?
Retry timer (mSec) [3000]?
```

Nota: El valor que sigue inmediatamente al indicador de opción de mandato es el valor actual de esta opción. No es siempre el valor por omisión ilustrado en este capítulo.

Retry timer

Establece el período de tiempo en milisegundos que transcurre antes de que la transmisión que hace LCP de los paquetes de petición de configuración (para abrir el enlace) y de petición de terminación (para cerrar el enlace) exceda el tiempo de espera. El vencimiento de este temporizador provoca una situación de tiempo de espera excedido y la parada de la transmisión de paquetes de petición de configuración y de petición de terminación. El rango es de 200 a 30000 milisegundos. El valor por omisión es 3000 milisegundos.

Config tries

Establece el número de veces que LCP envía paquetes de petición de configuración a una estación similar para establecer la apertura de un enlace PPP. El valor por omisión es 20. El rango es de 1 a 100.

El temporizador de reintentos se inicia después de transmitir el primer paquete de petición de configuración. Esto se hace como defensa contra la pérdida de paquetes.

NAK tries

Establece el número de veces que LCP envía paquetes de no

Configuración de interfaces PPP (Talk 6)

reconocimiento de configuración (nak = sin reconocimiento) a una estación similar mientras intenta abrir un enlace PPP. El valor por omisión es 10. El rango es de 1 a 100.

LCP envía paquetes de no reconocimiento de configuración en la recepción de paquetes de petición de configuración con algunas opciones de configuración no aceptables. Estos paquetes se envían para rechazar las opciones de configuración ofrecidas y para sugerir valores modificados, aceptables.

Terminate tries

Establece el número de veces que LCP envía paquetes de petición de terminación a una estación similar para cerrar un enlace PPP. El valor por omisión es 10. El rango es de 1 a 100.

El temporizador de reintentos se inicia después de transmitir el primer paquete de petición de terminación. Esto se hace como defensa contra la pérdida de paquetes.

name Establece el nombre que el direccionador utiliza cuando responde a las peticiones de autenticación de otro direccionador.

Notas:

1. Aunque las “mayúsculas/minúsculas” que se utilizan para los nombres y contraseñas enviados al similar en el enlace se conservan para este producto, la interoperatividad con los productos de otros proveedores es más fácil si todos los nombres y contraseñas se entran en *minúsculas*.
2. Es posible que otras implementaciones no manejen nombres con la misma longitud máxima que la soportada en este producto. La única indicación es un mensaje del autenticador indicando que hay un nombre incorrecto. Si recibe este tipo de mensaje, intente reducir el ID de direccionador.
3. Este mandato establece el nombre del direccionador local. Utilice el mandato **add ppp-user** de talk 6 en el indicador Config> para añadir cada usuario remoto a la base de datos local, si desea utilizar la base de datos local para hacer un seguimiento de los usuarios remotos. La alternativa es configurar el servidor externo de autenticación AAA que se describe en el capítulo “Utilización de autenticación local o remota” de la publicación *Utilización y configuración de las características*.

Nota: MS-CHAP no puede utilizar el servidor externo de autenticación AAA.

Ejemplo:

```
set name
PPP 7 Config>set name
Enter Local Name: [ ]? newyork
Password:
Enter password again:
PPP Local Name = newyork
```

ncp parameters

Establece los parámetros operativos básicos para la mayoría de NCP.

Nota: Aunque se accede a este mandato a través de una interfaz en particular, este mandato restablecerá los parámetros para todas las interfaces PPP.

Ejemplo:

```
set ncp parameters
Config tries [20]
NAK tries [10]?
Terminate tries [10]?
Retry timer (mSec) [3000]?
```

Config tries

Establece el número de paquetes de petición de configuración enviados por NCP a una estación similar para intentar abrir un enlace PPP. El rango es de 1 a 100. El valor por omisión es 20.

Esta acción indica el deseo de abrir una conexión NCP con un conjunto de opciones de configuración especificadas. El temporizador de reintentos se inicia después de transmitirse un paquete de petición de configuración. Esto se hace como defensa contra la pérdida de paquetes.

NAK tries

Establece el número de paquetes de no reconocimiento (nak) de configuración que NCP envía a una estación similar mientras intenta abrir un enlace PPP. El rango es de 1 a 100. El valor por omisión es 10.

En la recepción de paquetes de petición de configuración con algunas opciones de configuración no aceptables, NCP envía paquetes de no reconocimiento de configuración. Estos paquetes se envían para rechazar las opciones de configuración ofrecidas y para sugerir valores modificados, aceptables.

Terminate tries

Establece el número de paquetes de petición de terminación enviados por NCP a una estación similar para cerrar un enlace PPP. El rango es de 1 a 100. El valor por omisión es 10.

Esta acción indica el deseo de cerrar una conexión NCP. El temporizador de reintentos se inicia después de transmitirse un paquete de petición de terminación. Esto se hace como defensa contra la pérdida de paquetes.

Retry timer

Establece el período de tiempo, en milisegundos, que transcurre antes de que la transmisión que hace NCP de paquetes de petición de configuración (para abrir el enlace) y de petición de terminación (para cerrar el enlace) excedan el tiempo de espera. El vencimiento de este temporizador provoca una situación de tiempo de espera excedido y la parada de la transmisión de paquetes de petición de configuración y de petición de terminación. El rango es de 200 a 30000 milisegundos. El valor por omisión es de 3000 milisegundos.

Acceso al proceso de supervisión de interfaces

Para acceder al proceso de supervisión de interfaces PPP, lleve a cabo lo siguiente:

1. Entre **interface** en el indicador + para visualizar una lista de las interfaces configuradas.
2. Entre **network** seguido del número de la interfaz PPP.

```
+ network 2
PPP>
```

Mandatos de supervisión Point-to-Point

Esta sección resume y explica los mandatos de supervisión Point-to-Point. Entre los mandatos en el indicador PPP>. La Tabla 82 muestra los mandatos.

Nota: Las opciones disponibles para estos mandatos dependen de los protocolos disponibles en el software del direccionador. Por ejemplo, cuando el software del direccionador (imagen) no contiene el soporte APPN, los mandatos **list isrcp**, **list isr**, **list hprcp**, **list hpr** y **llc** no están disponibles.

Tabla 82. Resumen de los mandatos de supervisión Point-to-Point

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado "Cómo obtener ayuda" en la página 10.
Clear	Borra todas las estadísticas de las interfaces de punto a punto.
List	Visualiza la información y los contadores relacionados con la interfaz de punto a punto y los parámetros y opciones PPP.
LLC	Visualiza el indicador de supervisión LLC.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página 11.

Clear

Utilice el mandato **clear** para borrar todas las estadísticas de las interfaces de punto a punto.

Sintaxis:

clear all

Ejemplo: clear all

List

Utilice el mandato **list** para visualizar la información y los contadores relacionados con la interfaz de punto a punto y los parámetros y opciones PPP.

Sintaxis:

list all
cbcp - callback cp
control
errors
interface
lcp - PPP link CP
pap - PAP Authentication CP
chap - CHAP Authentication CP
mschap - MS-CHAP Authentication CP
ecp - Encryption Control Protocol
edp - Encrypted packet statistics
mppe - Microsoft PPP Encryption (MPPE)

Supervisión de interfaces PPP (Talk 5)

spap - SPAP Authentication CP
ccp - PPP Compression CP
cdp - PPP compression
compression - PPP compression
bcp - Bridging (ASRT) CP
brg - Bridging (ASRT)
stp - Spanning Tree Protocol
nbcpc - NetBios
nbfcpc - NetBios Frame
ipcp - Internet Protocol CP
ip - Internet Protocol
ipv6cp - Internet Protocol versión 6 CP
ipv6 - Internet Protocol versión 6
ipxcp - Novell IPX CP
ipx - Novell IPX
atcp - AppleTalk (Phase 2) CP
ap2 - AppleTalk (Phase 2)
dncpc - DECnet IV CP
dn - DECnet IV
osicpc - ISO's OSI CP
osi - ISO's OSI
bvcpc - Banyan VINES CP
vines - Banyan VINES
isrcpc - APPN ISR CP
isr - APPN ISR
hprcpc - APPN HPR CP
hpr - APPN HPR

all Lista toda la información y los contadores relacionados con la interfaz de punto a punto y las opciones y parámetros PPP. La salida visualizada para este mandato es una combinación de todas las visualizaciones de todos los mandatos **list elemento** individuales.

Nota: Si un protocolo de control de red no está disponible en una interfaz, se visualiza un mensaje indicando que no hay ninguna información de protocolo ni de estadísticas disponible para los mandatos **list** de este protocolo de control de red.

cbcp Lista las estadísticas para el protocolo Callback Control.

Ejemplo: list cbcp

Supervisión de interfaces PPP (Talk 5)

```
CBCP Statistics          In          Out
-----
Packets:                0            0
Octets:                 0            0
Callback attempts:      0
Successful callbacks:   0
```

Packets

Indica el número total de paquetes CBCP transmitidos (out) y recibidos (in) a través de la interfaz de punto a punto actual.

Octets

Para las tramas CBCP, indica el número total de bytes en los octetos transmitidos y recibidos a través de la interfaz de punto a punto actual.

Callback attempts

El número de llamadas de retorno CBCP intentadas, incluidas las que están en proceso.

Successful callbacks

El número de llamadas de retorno satisfactorias completadas.

control

Lista las opciones negociadas u otra información de estado para un protocolo de control.

```
ccp
ecp
lcp
bcp
nbcP
nbfcP
ipcp
ipxcp
atcp
dnCP
osicP
bvcp
isrcP
hprcp
```

Ejemplos del mandato list control ccp

Ejemplo para STAC-LZC:

```
list control ccp
CCP State:                Open
Previous State:           Ack Sent
Time Since Change:        264 hours, 56 minutes and 58 seconds

Compressor:  STAC-LZS histories 1, check_mode SEQ
Decompressor: STAC-LZS histories 1, check_mode SEQ

MPPE : Negotiated 40 bit stateful
```

Ejemplo para MPPC:

```
list control ccp
CCP State      :      Open
Previous State :      Listen
Time Since Change:    167 minutes

Compressor : none
```

Supervisión de interfaces PPP (Talk 5)

Decompressor : none

MPPE : Negotiated 40 bit stateful

Definiciones de los términos del ejemplo de list control ccp

CCP state

El estado actual del enlace de punto a punto. Si es "Open", la compresión se ha negociado satisfactoriamente en este enlace. Si no está abierto, la compresión no se ejecuta en el enlace. También aparecerá como "Open" si MPPE se ha negociado satisfactoriamente.

Previous State

Estado del enlace de punto a punto antes del estado visualizado en el campo de estado actual.

Compressor

Muestra qué compresor se ha negociado y las opciones que utiliza.

Decompressor

Muestra qué descompresor se ha negociado y las opciones que utiliza.

MPPE Las opciones MPPE negociadas. Consulte el mandato **enable mppe** de talk 6 para ver las descripciones de estos parámetros y la sección Microsoft Point-to-Point Encryption (MPPE) en el capítulo "Utilización y configuración de protocolos de encriptación" de la publicación *Utilización y configuración de las características* para obtener más información.

Ejemplo de mandato list control ecp

Ejemplo:

```
PPP x>list control ecp
```

```
ECP State:          Open
      Previous State:          Ack Sent
Time Since Change:  16 minutes and 40 seconds
Local (transmit) encrypter: DES
Remote (receive) encrypter: DES
```

Definiciones de los términos del ejemplo de list control ECP

ECP State:

El estado actual del enlace de punto a punto. Si es "Open", se ha negociado satisfactoriamente el cifrado en este enlace. Si no es "Open", el cifrado no se ejecuta en el enlace.

Nota: El soporte de cifrado es opcional y debe añadirse a la carga de software utilizando el mandato **load add**. Consulte la sección "Load" en la página 101.

Previous State:

El estado del enlace de punto a punto antes del estado visualizado en el campo de estado actual.

Time Since Change:

El tiempo transcurrido entre los dos cambios de estado anteriores.

Local (transmit) encrypter:

Este algoritmo de cifrado se utiliza para cifrar los datos que se están enviando en esta interfaz PPP.

Supervisión de interfaces PPP (Talk 5)

Remote (receive) encrypter:

El algoritmo de cifrado se utiliza para descifrar los datos recibidos en esta interfaz.

Ejemplo de mandato list control lcp

Ejemplo:

```
list control lcp
```

```
Version:                1
Link phase:            Establishing connection (LCP)
LCP State:             Listen
Previous State:        Req Sent
Time Since Change:     1 minute and 57 seconds
Remote Username:       - No Authentication -
Last Identification Rx'd
Time Connected:        - No Connection -

LCP Option             Local             Remote
-----
Max Receive Unit:      2048             1500
Async Char Mask:       FFFFFFFF          FFFFFFFF
Authentication:        None             None
Magic Number:          7A8CBFD7          None
Protocol Field Comp:   No                No
Addr/Cntl Field Comp: No                No
32-Bit Checksum:       No                No
```

Definiciones de los términos del ejemplo de list control lcp

Version

Visualiza la versión actual de Point-to-Point Protocol.

Link phase

Visualiza la actividad actual en el enlace. Puede tener uno de los valores siguientes:

Dead No hay actividad en el enlace; la interfaz está desactivada.

LCP El enlace está en negociación de LCP. Este estado se produce la primera vez que se activa una interfaz. La interfaz puede estar en la autopruueba en este momento.

Authenticate

El enlace está realizando la autenticación inicial.

ECP El enlace está negociando un algoritmo de cifrado ECP.

Nota: El soporte del cifrado es opcional y debe añadirse a la carga del software utilizando el mandato **load add**. Consulte el mandato **load** del proceso de configuración en el manual *Nways Multiprotocol Access Services Guía del usuario de software*.

El uso del cifrado múltiple (utilizar el cifrado en la Capa de seguridad de IP y en la Capa de enlace de datos de PPP o Frame Relay) en el direccionador está restringido por la legislación de exportación del Gobierno de los Estados Unidos. Sólo está soportado en cargas de software bajo un estricto

Supervisión de interfaces PPP (Talk 5)

control de la exportación (cargas de software que dan soporte a RC4 con claves de 128 bits y DES triple).

Ready El enlace está funcionando normalmente. Los NCP pueden negociar y el tráfico de datos asociado puede fluir después de una negociación NCP satisfactoria.

Terminate

El enlace se está cerrando.

LCP State

Visualiza el estado actual del enlace de punto a punto. Estos estados incluyen los siguientes:

OPEN - Indica que se ha establecido una conexión y que se pueden enviar datos. El temporizador de reintentos no se ejecuta en este estado.

CLOSED - Indica que el enlace está desactivado y que no se está intentando abrirlo. En este estado, se rechazan todas las peticiones de conexión de los similares.

LISTEN - Indica que el enlace está desactivado y que no se está intentando abrirlo. Sin embargo, a diferencia del estado **CLOSED**, se aceptan todas las peticiones de conexión de los similares.

REQUEST-SENT - Indica que se está efectuando un intento activo de abrir el enlace. Se ha enviado un paquete de Petición de configuración pero no se ha recibido todavía un Reconocimiento de configuración ni se ha enviado ninguno. El temporizador de reintentos está en ejecución en este momento.

ACK-RECEIVED - Indica que se ha enviado un paquete de Petición de configuración y que se ha recibido un paquete de Reconocimiento de configuración. El temporizador de reintentos sigue en ejecución ya que no se ha transmitido ningún Reconocimiento de configuración.

ACK-SENT - Indica que se ha enviado un paquete de Reconocimiento de configuración y un paquete de Petición de configuración pero no se ha recibido ningún paquete de Reconocimiento de configuración. El temporizador de reintentos se ejecuta siempre en este estado.

CLOSING - Indica que se está intentando cerrar la conexión. Se ha enviado un paquete de Petición de terminación pero no se ha recibido ningún paquete de Reconocimiento de terminación. El temporizador de reintentos se ejecuta en este estado.

Previous State

Visualiza el estado del enlace de punto a punto antes del estado visualizado en el campo de estado actual. Estos estados son los mismos que los descritos en el campo de estado actual.

Time since change

Visualiza el período de tiempo que ha transcurrido desde el último cambio de estado del enlace.

Remote Username

Cuando es necesaria la autenticación en el enlace, este campo muestra el nombre que el similar ha suministrado.

Supervisión de interfaces PPP (Talk 5)

Last Identification Rx'd

Un tipo de paquete opcional que se define para LCP es un paquete de "Identificación". El contenido de este paquete es indefinido, pero normalmente se espera que sea una serie que el hombre puede leer proporcionada por el similar para facilitar alguna información de identificación como, por ejemplo, un nombre, fabricante, el número de modelo u otra información que el fabricante desee proporcionar. Si el direccionador recibe un paquete así, se visualiza el contenido del último paquete como este que se ha recibido.

Time Connected

Indica el período de tiempo que el similar ha estado conectado en este enlace.

LCP Option

Estos campos indican los valores de las opciones que se han negociado con el similar cuando LCP está en el estado Open (abierto). Cuando LCP no está abierto, estos valores representan los valores por omisión iniciales o los valores configurados que se utilizarán en negociaciones subsiguientes de LCP.

Max Receive Unit

Indica la longitud máxima para el tamaño de paquete que los extremos local y remoto pueden transmitir. Esta es la longitud máxima de la porción de carga útil de un paquete PPP y no incluye los bytes de cabecera ni de cola de PPP.

Cuando LCP está en estado Open, los valores indican las longitudes que se han negociado con el similar. El direccionador no soporta las diferencias de longitud de MRU para el similar y el extremo local, de modo que estos valores serán los mismos.

Async Character Mask

Esto indica la máscara de caracteres de control asíncrona que se ha negociado. El direccionador acepta la negociación ACCM incluso en líneas síncronas, aunque no afecta a los datos reales del paquete enviados. Consulte el mandato **set lcp options** en la página 657 para obtener más información acerca de ACCM.

Authentication

Indica qué protocolo de autenticación, si hay alguno, necesita cada extremo del enlace. Pueden estar disponibles múltiples protocolos en cada extremo; este valor indica qué protocolo han acordado utilizar las unidades.

Magic number

Visualiza el número mágico actual que se está utilizando para los extremos local y remoto del enlace para la detección de bucles de retorno.

Protocol compression

Indica si se ha negociado PFC.

Address/Control compression

Indica si se ha negociado ACFC.

32-bit checksum

No se soporta actualmente. PPP rechazará esta opción si se recibe.

Ejemplo del mandato list control bcp

Ejemplo:

```
list control bcp
BCP State:          Closed
Previous State:     Closed
Time Since Change:  5 hours, 25 minutes and 3 seconds

BCP Option          Local          Remote
Tinygram Compression  DISABLED        DISABLED
Source-route Info:
Remote side does not support source-route bridging
```

Definiciones de los términos del ejemplo de list control bcp

Los campos de estado de BCP son los mismos que los descritos bajo el mandato **list control lcp**.

Tinygram Compression

Visualiza si está habilitada o no la Compresión de tinygramas en los extremos local y remoto del enlace.

Source-route Info

Visualiza si está habilitado o no el puente de ruta de origen para los puertos local y remoto que corresponden a esta interfaz.

Ejemplo del mandato list control nbcp

Ejemplo:

```
list control nbcp
NBFCP State:          Closed
Previous State:       Closed
Time Since Change:    4 hours, 5 minutes and 58 seconds

NetBIOS Frame Control Protocol Info:
Local MAC Address = 0x000000000000
Remote MAC Address = 0x444553540000
Remote NetBIOS Names: (0)

Remote Peer Class:    0
Remote Peer Version Major: 0
Remote Peer Version Minor: 0
```

Definiciones de los términos del ejemplo list control nbcp

Los campos de estado de NBFCP son los mismos que los descritos bajo el mandato **list control lcp**.

Local MAC Address

La dirección MAC local es la dirección MAC que utiliza el cliente Win 95/NT Dial-Up Networking. Es un número pseudoaleatorio o una Dirección administrada localmente (LAA), si ha configurado una LAA en el cliente.

Remote MAC Address

La dirección MAC remota es la Dirección MAC que el 2216 Servidor DIAL ha asignado a este cliente para utilizar en la LAN.

Remote NetBIOS Name

La lista de nombres NetBIOS de los recursos LAN a los que el cliente ha pedido acceder.

Supervisión de interfaces PPP (Talk 5)

Remote Peer

Remote Peer Class, Version Major y Version Minor es la información devuelta al 2216 por la opción Peer Information de NBFCP.

Ejemplo del mandato list control ipcp

Ejemplo:

```
list control ipcp
IPCP State:          Listen
Previous State:      Closed

Time Since Change:   3 minutes and 40 seconds

IPCP Option          Local          Remote
-----
IP Address           0.0.0.0          None
TCP Compression Slots 16              None
Non-TCP Compression Slots 16             None

DNS servers obtained from remote:
  Primary DNS:  None
  Secondary DNS: None

DHCP State:          BOUND
Lease Server:        10.0.0.111
Leased IP Address:   10.0.0.152
Lease Time:          4 minutes and 0 seconds
Renewal Time:        2 minutes and 0 seconds
Rebind Time:         3 minutes and 30 seconds
Lease Time Elapsed:  1 second
Lease Time Remaining: 3 minutes and 59 seconds

DHCP Client ID:      0100120B0000
```

Definiciones de los términos del ejemplo de list control ipcp

Los campos de estado de IPCP son los mismos que los descritos bajo el mandato **list control lcp**.

IP Address:

Indica la dirección IP (Local) configurada o negociada de esta interfaz y la dirección negociada remota (Remote), si la hay.

TCP Compression Slots

Estas ranuras sólo son para el tráfico TCP.

Non-TCP Compression Slots

Estas ranuras sólo son para el tráfico que no es TCP.

DNS servers obtained from remote

Indica las direcciones IP de los Servidores de nombres de dominio (DNS) proporcionadas por la parte remota.

DHCP State

Se trata de DHCP proxy tal como se describe en RFC 1541.

Lease Server

El servidor del que se ha adquirido el alquiler.

Leased IP address

La dirección alquilada al cliente. Esta dirección debe ser equivalente a "Remote IP Address" de la lista anterior.

Lease Time

Duración del alquiler del servidor DHCP para esta dirección. Cuando "Lease Time Elapsed" es igual a este tiempo, el alquiler caducará y se cerrará la conexión IPCP.

Renewal Time

Período de tiempo después del cual DHCP proxy intenta ampliar este alquiler del servidor. Cuando "Lease Elapsed Time" es igual a este tiempo, DHCP proxy intenta renovar el alquiler, restableciendo "Lease Time," "Lease Elapsed Time" y "Lease Time Remaining," si es satisfactorio.

Rebind Time

Tiempo antes del cual DHCP proxy intenta obtener un nuevo alquiler de cualquier servidor DHCP configurado. Cuando "Lease Elapsed Time" es igual a este tiempo, DHCP proxy intenta obtener un nuevo alquiler, restableciendo "Lease Time," "Lease Elapsed Time" y "Lease Time Remaining," si es satisfactorio.

Leased Time Elapsed

Período de tiempo transcurrido para este alquiler. No es necesariamente el tiempo para esta sesión de marcación de entrada en particular, ya que el alquiler puede haberse renovado. Cuando se renueva el alquiler, este temporizador se establece de nuevo en 0.

Leased Time Remaining

El tiempo que queda para este alquiler. Este parámetro es igual a "Lease Time" menos "Lease Time Elapsed."

DHCP client ID

Un ID exclusivo para este cliente (usuario de marcación de entrada). Todos los mensajes DHCP se identifican en el servidor DHCP por este ID de cliente.

Ejemplo del mandato list control ipxcp

Ejemplo:

```
list control ipxcp
IPXCP State:      Closed
Previous State:   Closed
Time Since Change: 2 hours, 9 minutes and 9 seconds
```

Los campos de estado de IPXCP son los mismos que los descritos bajo el mandato **list control lcp**. **Ejemplo del mandato list control atcp**

Ejemplo:

```
list control atcp
ATCP State:      Closed
Previous State:   Closed
Time Since Change: 6 hours, 27 minutes and 7 seconds

AppleTalk Address Info:
Common network number = 12
Local node ID = 49
Remote node ID = 76
```

Definiciones de los términos del ejemplo de list control atcp

Los campos de estado de ATCP son los mismos que los descritos bajo el mandato **list control lcp**.

Common Network Number

El número de red de los dos extremos del enlace de punto a punto. (Debe configurar estáticamente ambos extremos del enlace para que tengan el mismo número de red.)

Supervisión de interfaces PPP (Talk 5)

Local Node ID

El número de nodo exclusivo del extremo local del enlace.

Remote Node ID

El número de nodo exclusivo del extremo remoto del enlace.

Ejemplo:

```
list control dnpc
DNCP State:          Closed
Previous State:      Closed
Time Since Change:   2 hours, 2 minutes and 58 seconds
```

Los campos de estado de DNCP son los mismos que los descritos bajo el mandato **list control lcp**.

Ejemplo:

```
list control osicp
OSICP State:         Closed
Previous State:      Closed
Time Since Change:   6 hours, 28 minutes and 32 seconds
```

Los campos de estado de OSICP son los mismos que los descritos bajo el mandato **list control lcp**. **Ejemplo del mandato list control bvcp**

Ejemplo:

```
list control bvcp
BVCP State:          Open
Previous State:      Ack Sent
Time Since Change:   403 hours, 49 minutes and 2 seconds
```

Los campos de estado de BVCP son los mismos que los descritos bajo el mandato **list control lcp**.

Nota: La palabra **bvcp** del mandato y el acrónimo BVCP significan Banyan VINES Control Protocol (BVCP).

Ejemplo del mandato list control isrcp

Ejemplo:

```
list control isrcp
APPN ISRCP State:    Open
Previous State:      Ack Rcvd
Time Since Change:   1 hour, 48 minutes and 5 seconds
```

Los campos de estado del protocolo de control APPN ISR (ISRCP) son los mismos que los descritos bajo el mandato **list control lcp**. **Ejemplo del mandato list control hprcp**

Ejemplo:

```
list control hprcp
APPN HPRCP State:    Open
Previous State:      Ack Rcvd
Time Since Change:   1 hour, 48 minutes and 10 seconds
```

Los campos de estado del protocolo de control APPN HPR (HPRCP) son los mismos que los descritos bajo el mandato **list control lcp**

error Lista la información relacionada con todas las condiciones de error seguidas por el software PPP.

Ejemplo:

```
list error
Error Type          Count      Last One
-----
Bad Address:        0          0
```

Supervisión de interfaces PPP (Talk 5)

Bad Control:	0	0
Unknown Protocol:	0	0
Invalid Protocol:	0	0
Config Timeouts:	0	0
Terminate Timeouts:	0	0

Bad address

Indica el número total de direcciones incorrectas encontradas en el enlace de punto a punto. "Bad addresses" hace referencia al byte de trama HDLC al principio del paquete.

Bad control

Indica el número total de paquetes de control incorrectos que se han encontrado en el enlace de punto a punto. "Bad control" hace referencia al prefijo 0x03 de los paquetes PPP encapsulados HDLC (el valor "UI" que sigue a 0xFF).

Unknown protocol

Indica el número total de paquetes de protocolo desconocido encontrados por el enlace actual.

Invalid protocol

Indica el número total de paquetes de protocolo no válidos encontrados por el enlace actual.

Config timeouts

Indica el número total de tiempos de espera excedidos experimentados por el enlace.

Terminate timeouts

Indica el número total de tiempos de espera excedidos de terminación de enlace encontrados por el enlace.

interface

Lista las estadísticas de interfaz PPP.

Ejemplo:

```
list interface
Interface Statistic      In      Out
-----
Packets:                 0        0
Octets:                  0        0
```

Packets

Indica el número de paquetes recibidos y transmitidos en esta interfaz.

Octets

Indica el número de octetos recibidos y transmitidos en esta interfaz.

lcp

Lista las estadísticas para Link Control Protocol.

Ejemplo:

```
list lcp
LCP STATISTIC          IN      OUT
-----
PACKETS:               42      42
OCTETS:                1260    1260
CFG REQ:               0        0
CFG ACK:               0        0
CFG NAK:               0        0
CFG REJ:               0        0
TERM REQ              0        0
TERM ACK              0        0
ECHO REQ:             21      21
ECHO RESP:            21      21
DISC REQ:             0        0
CODE REJ:             0        0
```

Supervisión de interfaces PPP (Talk 5)

Packets

Indica el número total de paquetes LCP transmitidos (out) y recibidos (in) a través de la interfaz de punto a punto actual.

Octets

Para las tramas LCP, indica el número total de bytes en octetos transmitidos y recibidos a través de la interfaz de punto a punto actual.

CFG REQ

Indica el número total de paquetes LCP de petición de configuración transmitidos y recibidos a través de la interfaz de punto a punto actual.

CFG ACK

Indica el número total de paquetes LCP de reconocimiento de configuración transmitidos y recibidos a través de la interfaz de punto a punto actual.

CFG NAK

Indica el número total de paquetes LCP de no reconocimiento (nak) de configuración transmitidos y recibidos a través de la interfaz de punto a punto actual.

CFG REJ

Indica el número total de paquetes LCP de rechazo de configuración transmitidos y recibidos a través de la interfaz de punto a punto actual.

TERM REQ

El número total de paquetes LCP de petición de terminal transmitidos y recibidos a través de la interfaz de punto a punto actual.

TERM ACK

El número total de paquetes LCP de reconocimiento de terminal transmitidos y recibidos a través de la interfaz de punto a punto actual.

ECHO REQ

Indica el número total de paquetes LCP de petición de eco transmitidos y recibidos a través de la interfaz de punto a punto actual.

ECHO RESP

Indica el número total de paquetes LCP de respuesta de eco transmitidos y recibidos a través de la interfaz de punto a punto actual.

DISC REQ

Indica el número total de paquetes LCP de petición de eliminación transmitidos y recibidos a través de la interfaz de punto a punto actual.

CODE REJ

Indica el número total de paquetes LCP de rechazo de código transmitidos y recibidos a través de la interfaz de punto a punto actual.

pap Lista las estadísticas para Password Authentication Protocol.

Ejemplo:

Supervisión de interfaces PPP (Talk 5)

```
list pap
PAP Statistics
-----
Packets:      0          0
Octets:       0          0
Requests:     0          0
Acks:         0          0
Naks:         0          0
```

Packets

El número total de paquetes PAP enviados o recibidos.

Octets

El número de bytes de datos que se han enviado o recibido en estos paquetes.

Requests

El número de paquetes de “Petición” PAP enviados o recibidos. Estos son los paquetes que contienen los pares de nombre/contraseña PAP.

Acks El número de Reconocimientos (respuestas satisfactorias) enviados o recibidos para las peticiones PAP (por ejemplo, si el similar envía un paquete de petición válido, el direccionador responde con un reconocimiento).

Naks El número de No reconocimientos enviados o recibidos para las peticiones PAP (por ejemplo, si el similar envía un paquete de Petición no válido, el direccionador responde con un No reconocimiento).

chap Lista las estadísticas para Challenge-Handshake Authentication Protocol.

Ejemplo:

```
list chap
CHAP Statistics
-----
Packets:      0          0
Octets:       0          0
Challenges:   0          0
Responses:    0          0
Successes:    0          0
Failures:     0          0
```

Packets

El número total de paquetes CHAP enviados o recibidos.

Octets

El número de bytes de datos que se han enviado o recibido en los paquetes.

Challenges

El número de paquetes de “cuestión de la identidad” CHAP enviados o recibidos. Un paquete de cuestión de la identidad CHAP incluye una clave de cifrado generada aleatoriamente y es una petición al similar que genere una respuesta adecuada basándose en esa clave y en la información de contraseña almacenada.

Responses

El número de paquetes de “Respuesta” CHAP enviados o recibidos. Un paquete de respuesta contiene una respuesta del similar a una petición de “cuestión de la identidad”.

Successes/Failures

El número de paquetes satisfactorios o anómalos enviados o

Supervisión de interfaces PPP (Talk 5)

recibidos. Una unidad envía un paquete de cuestión de la identidad y espera la respuesta del similar. Después examina el paquete de respuesta y envía un paquete de satisfactorio o anómalo para indicar si la respuesta era válida.

Estos contadores reflejan el número de paquetes satisfactorios o anómalos enviados. Un similar puede realizar varios intentos para responder satisfactoriamente antes de que se considere que la autenticación ha fallado.

mschap

Lista las estadísticas MS-CHAP para cada dirección.

Packets

Número total de paquetes MS-CHAP.

Octets

Número total de bytes contenidos en paquetes MS-CHAP.

Challenges

Número de paquetes de cuestión de la identidad MS-CHAP.

Responses

Número de paquetes de respuesta MS-CHAP.

Successes

Número de paquetes satisfactorios MS-CHAP.

Failures

Número de paquetes anómalos MS-CHAP.

Failure: Restricted Hours

Número de paquetes de anomalía enviados debido al intento del usuario PPP de acceder al 2216 fuera de las horas permitidas de ese usuario. Este contador no está soportado y siempre será 0.

Failure: Account Disabled

Número de paquetes de anomalía enviados debido a que se ha inhabilitado el ID del usuario PPP en el 2216.

Failure: Password Expired

Número de paquetes de anomalía enviados porque ha caducado la contraseña del usuario PPP.

Failure: No Dialin Permission

Número de paquetes de anomalía enviados porque el usuario PPP no está autorizado para llamar a este 2216.

Failure: Authentication

Número de paquetes de anomalía enviados porque las credenciales del usuario PPP (ID o contraseña) no se reconocen en el 2216.

Failure: Change Password

Número de paquetes de anomalía enviados como resultado de un error encontrado al procesar el paquete de Cambio de contraseña.

Change Password

Número de paquetes de cambio de contraseña. El direccionador no enviará nunca un paquete de cambio de contraseña; por lo tanto, el contador de salida siempre será 0.

ecp

Lista las estadísticas para los paquetes ECP (protocolo de control de cifrado) enviados o recibidos en la interfaz.

Ejemplo:

PPP x>list ecp

ECP Statistic	In	Out
-----	--	---
Packets:	2	2
Octets:	26	26
Reset Reqs:	0	0
Reset Acks:	0	0
Prot Rejects:	0	-
Local (transmit) encrypter: DES		
Remote (receive) encrypter: DES		

Nota: El soporte de cifrado es opcional y debe añadirse a la carga de software utilizando el mandato **load add**. Consulte la sección “Load” en la página 101.

Packets

Indica el número total de paquetes ECP transmitidos (out) y recibidos (in) a través de la interfaz de punto a punto actual.

Octets

Indica el número total de bytes transmitidos y recibidos en los paquetes ECP.

Reset Reqs

Indica el número de peticiones de restablecimiento transmitidas y recibidas en esta interfaz. Se enviará una petición de restablecimiento siempre que ECP elimine un paquete EDP.

Nota: Puesto que DES, el único algoritmo de cifrado soportado, no envía peticiones de restablecimiento, este número será cero.

Reset Acks

Indica los reconocimientos de restablecimiento transmitidos y recibidos en esta interfaz. Se enviará un paquete de Reconocimiento de restablecimiento para cada paquete de Petición de restablecimiento recibido.

Nota: Puesto que DES, el único algoritmo de cifrado soportado, no envía ninguna Petición de restablecimiento, este número será cero.

Prot Rejects

Indica el número total de paquetes de rechazo de protocolo transmitidos y recibidos a través de la interfaz de punto a punto actual.

Local (transmit) encrypter

Este algoritmo de cifrado se utilizará para cifrar los datos que se envían en esta interfaz de punto a punto.

Remote (receive) encrypter

Este algoritmo de cifrado se utilizará para descifrar los datos recibidos en esta interfaz de punto a punto.

edp Lista las estadísticas asociadas con los paquetes cifrados ECP que se envían o reciben en la interfaz.

Ejemplo:

PPP x>list edp

Encryption Statistic	In	Out
-----	--	---
Packets:	20	30
Octets:	29164	44790

Supervisión de interfaces PPP (Talk 5)

Encrypted Octets:	29280	44880
Discarded Packets:	0	0
Prot Rejects:	0	-

Nota: El soporte de cifrado es opcional y debe añadirse a la carga de software utilizando el mandato **load add**. Consulte la sección “Load” en la página 101.

Packets

Indica el número total de paquetes IP transmitidos (out) y recibidos (in) a través de la interfaz de punto a punto actual.

Octets

Indica el número total de octetos de bytes de datos transmitidos y recibidos a través de la conexión IP actual.

Encrypted Octets

Indica el número de octetos cifrados transmitidos o recibidos en esta interfaz.

Discarded Packets

Indica el número de paquetes que se eliminan debido a que no han podido descifrarse satisfactoriamente.

Prot Rejects

Indica el número total de paquetes de rechazo de protocolo transmitidos y recibidos a través de la interfaz de punto a punto actual.

mppe Visualiza las estadísticas de datos de cifrado para la configuración Microsoft PPP Encryption (MPPE).

Ejemplo:

```
list mppe
MPPE Statistic      In      Out
-----
Encrypted Octets :   0      0
Encrypted Packets :   0      0
Discarded Packets :   0      0
```

spap Lista las estadísticas para Shiva Password Authentication Protocol.

Ejemplo:

```
list spap
SPAP Statistic      In      Out
-----
Packets:            0      0
Octets:              0      0
Requests:           0      0
Acks:                0      0
Naks:                0      0
Dialbacks:          0      0
PleaseAuthenticates: 0      0
Change Passwords:   0      0
Alerts:              0      0
MCCP Call Reqs     0      0
MCCP Callbacks     0      0
MCCP ACKs           0      0
MCCP NAKs           0      0
```

Packets

El número total de paquetes SPAP enviados o recibidos.

Octets

El número de bytes de datos que se han enviado o recibido en estos paquetes.

Requests

El número de paquetes de "Petición" SPAP enviados o recibidos. Estos son los paquetes que contienen los pares de nombre/contraseña SPAP.

Acks El número de Reconocimientos (respuestas satisfactorias) enviados o recibidos para las peticiones SPAP (por ejemplo, si el similar envía un paquete de petición válido, el direccionador responde con un Reconocimiento).

Naks El número de No reconocimientos enviados o recibidos para las peticiones SPAP (por ejemplo, si el similar envía un paquete de petición no válido, el direccionador responde con un No reconocimiento).

Dialbacks

El número de veces que un usuario:

- Ha pedido una llamada de retorno (llamada de retorno voluntaria) y se le ha otorgado.
- Ha marcado y estaba configurado para la llamada de retorno necesaria y ha devuelto la llamada a un número predeterminado almacenado en el perfil de usuario.

PleaseAuthenticates

El número de paquetes de autenticación de gracia SPAP que se han enviado o recibido en esta interfaz. Un paquete de autenticación de gracia SPAP se envía como resultado de un tiempo de espera excedido cuando se espera que el otro extremo envíe una petición autenticación SPAP.

Change Passwords

El número de peticiones de cambio de contraseña que se han enviado o recibido en esta interfaz.

Alerts El numero de mensajes de cabecera SPAP que se han enviado o recibido.

MCCP Call Reqs

Indica que el emisor ha pedido otro número de teléfono para establecer un segundo enlace MP.

MCCP Callbacks

Indica que el emisor ha suministrado un número de teléfono al que se ha de llamar para establecer un segundo enlace MP.

MCCP ACKs

El número de reconocimientos enviados o recibidos por MCCP.

MCCP NAKs

El número de reconocimientos negativos enviados o recibidos por MCCP.

ccp Lista las estadísticas para el protocolo de control de la compresión.

Ejemplo:

```
list ccp
CCP  Statistic      In      Out
-----
Packets:           24      25
Octets:            174     177
Reset Reqs         0        0
Reset Acks:        0        0
Prot Rejects:      0        0
```

Supervisión de interfaces PPP (Talk 5)

Packets

Indica el número de paquetes recibidos y transmitidos en esta interfaz.

Octets

Indica el número de octetos recibidos y transmitidos en esta interfaz.

Reset Reqs

El número de "Peticiónes de restablecimiento" de diccionario CCP que se han enviado o recibido.

Reset Acks

El número de "Reconocimientos de restablecimiento" de diccionario CCP que se han transmitido o recibido.

Los paquetes de petición de restablecimiento y de Reconocimiento de restablecimiento son paquetes de control que se pasan entre las entidades CCP de cada extremo, utilizados para mantener la sincronización de los diccionarios de datos de cada extremo del enlace.

Prot Rejects

Indica el número de rechazos de protocolo de paquetes CCP enviados por el similar (la recepción de un rechazo de protocolo significaría que el similar no soporta CCP).

cdp Visualiza las estadísticas asociadas con los paquetes de datos comprimidos enviados o recibidos en esta interfaz.

Ejemplo:

```
list cdp
Compression Statistic      In              Out
-----
Packets:                   31035           46550
Octets:                    1614885        2421137
Compressed Octets:         931416         1521039
Incompressible Packets:    0               0
Discarded Packets:         0               0
Prot Rejects:              0               -
Compression Ratios         1.70            1.70
```

Packets

Estos contadores indican el número de datagramas comprimidos enviados y recibidos. En la parte de la salida, la cuenta sólo incluye los paquetes que se han enviado realmente como datagramas comprimidos PPP; no incluye los paquetes que se han encontrado que no se podían comprimir y se han enviado en su formato no comprimido original.

Estos contadores cuentan los paquetes enviados o recibidos que tenían el tipo de protocolo PPP X'00FD' (CDP). Cuando se ha negociado la modalidad de STAC ampliada o MPPC, los paquetes que no se pueden comprimir pueden encapsularse en datagramas CDP. Esta encapsulación incluiría los paquetes no comprimibles de estas cuentas.

Octets

Estos contadores indican el número de bytes que se han transmitido o recibido efectivamente en formato comprimido. Estos contadores reflejan las longitudes de los datagramas originales antes de la compresión o después de la descompresión.

Compressed octets

Estos contadores indican el número de bytes para todos los datagramas comprimidos enviados y recibidos. Estas cuentas son las longitudes de los paquetes CDP reales después de la compresión o antes de la descompresión.

Incompressible packets

Estos contadores indican el número de paquetes que no se han podido comprimir y que, por lo tanto, se han enviado en el formato original no comprimido.

Discarded packets

Estos contadores indican cuántos paquetes se han eliminado debido a que no se han podido descomprimir satisfactoriamente. Normalmente estos paquetes serán los paquetes que el similar estaba transmitiendo justo después de que el direccionador haya enviado una Petición de restablecimiento, pero antes de que el similar haya recibido y procesado la Petición de restablecimiento. También se eliminan los paquetes si el direccionador detecta que los datos de los paquetes son incorrectos. Un ejemplo de datos incorrectos es un paquete que contiene un número de secuencia incorrecto.

Si el número de paquetes eliminados aumenta demasiado rápidamente, es que se están perdiendo o dañando los paquetes en la línea, probablemente debido a ruido en la línea, y puede degradarse el rendimiento del enlace.

Protocol rejects

Este contador indica el número de paquetes de Rechazo de protocolo de CDP que se han recibido de un similar. Esta cuenta debe ser cero, porque el enlace no enviará paquetes CDP si la utilización de la compresión no se negoció todavía.

Compression ratios

Las proporciones facilitan una indicación aproximada de la eficacia del compresor y descompresor. Estas proporciones se basan en el número de bytes de texto plano dividido por el número de bytes comprimidos correspondiente, de modo que los valores mayores que 1 son preferibles para la entrada y la salida. Cuanto mayor sea el número, más eficaz será la compresión.

La proporción de salida se calcula como la proporción del número original de bytes de texto plano dividido por el número de bytes enviados como resultado del intento de compresión - se haya realmente comprimido el paquete o se haya enviado como un paquete CDP. Si una corriente de datos no comprime bien y la mayor parte de los paquetes se envían en su formato original o en paquetes CDP ampliados, la proporción de salida de compresión se desactivará. Si la proporción baja por debajo de 1,0, el compresor está realmente reduciendo la eficacia del ancho de banda de la línea en lugar de aumentarlo y debe inhabilitarse en esta interfaz si el estado persiste durante un período largo de tiempo.

La proporción de entrada se calcula basándose en el número de bytes recibidos en tramas CDP dividido por el número de bytes descomprimidos. A diferencia de la proporción de salida, esta cuenta no incluye ningún paquete que no se haya podido comprimir y se envía en formato de texto plano. Esto es debido a que el

Supervisión de interfaces PPP (Talk 5)

direccionador no puede determinar si un paquete no CDP recibido era un paquete no comprimible que el similar ha enviado en formato de texto plano o simplemente un paquete que el similar no ha intentado comprimir.

Debido al método de cálculo, la proporción de salida de un extremo del enlace no coincide necesariamente con la proporción de entrada del otro extremo.

compression

Este mandato visualiza la misma información que `list cdp`.

bcp Lista las estadísticas para el protocolo de control Bridging. Estos campos son los mismos que los descritos bajo el mandato `list ip`. (Consulte la sección “ip” en la página 683.)

Ejemplo:

```
list bcp
BCP Statistic      In      Out
-----
Packets:           0        0
Octets:            0        0
Prot Rejects:      0        -
```

brg Lista las estadísticas de los paquetes de puente recibidos y transmitidos a través de la interfaz PPP. Estos campos son los mismos que los descritos bajo el mandato `list ip`. (Consulte la sección “ip” en la página 683.)

Ejemplo:

```
list brg
BRG Statistic      In      Out
-----
Packets:           0        0
Octets:            0        0
Prot Rejects:      0        -
```

stp Lista las estadísticas para el protocolo de árbol de expansión. Estos campos son los mismos que los descritos bajo el mandato `list ip`. (Consulte la sección “ip” en la página 683.)

Ejemplo:

```
list stp
Spanning Tree Statistic  In      Out
-----
Packets:                 0        0
Octets:                  0        0
```

nbcpc Lista las estadísticas de NetBIOS Control Protocol para la interfaz de punto a punto. Estos campos son los mismos que los descritos bajo el mandato `list ip`. (Consulte la sección “ip” en la página 683.)

Ejemplo:

```
list nbcpc
NBCP Statistic      In      Out
-----
Packets:           0        0
Octets:            0        0
Prot Rejects:      0        -
```

nbfcpc Lista las estadísticas de NetBIOS Frame Control Protocol para la interfaz de punto a punto. Estos campos son los mismos que los descritos bajo el mandato `list ip`. (Consulte la sección “ip” en la página 683.)

Ejemplo:

```
list nbfcpc
NBFCP Statistic      In      Out
-----
Packets:           0        0
Octets:            0        0
Prot Rejects:      0        -
```

Supervisión de interfaces PPP (Talk 5)

ipcp Lista las estadísticas de Internet Protocol Control Protocol para la interfaz de punto a punto. Estos campos son los mismos que los descritos bajo el mandato **list ip**. (Consulte la sección “ip”.)

Ejemplo: Cuando se configura la Compresión de cabeceras RTP:

```
PPP 0>list ipcp
IPCP Statistic          In          Out
-----
Packets:                0           0
Octets:                 0           0
Prot Rejects:           0           -

RFC 2508 TCP/UDP/RTP Packet Statistics

Packet Type            TX          RX
-----
Full Headers           0           0
Compressed TCP         0           0
Compressed TCP No Delta 0           0

Compressed Non TCP     0           0
Compressed UDP         0           0
Compressed RTP         0           0
Context State          0           0

PPP 0>
```

Ejemplo: Cuando se configura la compresión de cabeceras VJ:

```
PPP 0>li ipcp
IPCP Statistic          In          Out
-----
Packets:                0           0
Octets:                 0           0
Prot Rejects:           0           -
```

ip Lista toda la información relacionada con los paquetes IP a través del enlace de punto a punto.

Ejemplo:

```
list ip
IP Statistic           In          Out
-----
Packets:               349         351
Octets:               128488     129412
Prot Rejects:         0           -
```

Packets

Indica el número total de paquetes IP transmitidos (out) y recibidos (in) a través de la interfaz de punto a punto actual.

Octets

Indica el número total de octetos transmitidos y recibidos a través de la conexión IP actual.

Prot Rejects

Indica el número total de paquetes de rechazo de protocolo transmitidos y recibidos a través de la interfaz de punto a punto actual.

ipv6cp

Lista las estadísticas del protocolo de control Internet Protocol versión 6 para la interfaz de punto a punto. Estos campos son los mismos que los descritos bajo el mandato **list ip**. (Consulte la sección “ip”.)

Ejemplo:

```
list ipv6cp
IPv6CP STATISTIC      IN          OUT
-----
PACKETS:              0           0
OCTETS:               0           0
PROT REJECTS:         0           0
```

Supervisión de interfaces PPP (Talk 5)

ipv6 Lista toda la información relacionada con los paquetes IPv6 a través del enlace de punto a punto. Estos campos son los mismos que los descritos bajo el mandato **list ip**. (Consulte la sección “ip” en la página 683.)

Ejemplo:

```
list ipv6
IPv6 Statistic      In      Out
-----
Packets:            0        0
Octets:             0        0
Prot Rejects:       0
```

ipxcp Lista las estadísticas para el protocolo de control IPX. Estos campos son los mismos que los descritos bajo el mandato **list ip**. (Consulte la sección “ip” en la página 683.)

Ejemplo:

```
list ipxcp
IPXCP Statistic     In      Out
-----
Packets:            0        0
Octets:             0        0
Prot Rejects:       0        -
```

ipx Lista las estadísticas de IPX para la interfaz de punto a punto. Estos campos son los mismos que los descritos bajo el mandato **list ip**. (Consulte la sección “ip” en la página 683.)

Ejemplo:

```
list ipx
IPX Statistic       In      Out
-----
Packets:            0        0
Octets:             0        0
Prot Rejects:       0        -
```

atcp Lista las estadísticas para el protocolo de control AppleTalk. Estos campos son los mismos que los descritos bajo el mandato **list ip**. (Consulte la sección “ip” en la página 683.)

Ejemplo:

```
list atcp
ATCP Statistic      In      Out
-----
Packets:            0        0
Octets:             0        0
Prot Rejects:       0        -
```

ap2 Lista las estadísticas de AppleTalk Phase 2 para la interfaz de punto a punto. Estos campos son los mismos que los descritos bajo el mandato **list ip**. (Consulte la sección “ip” en la página 683.)

Ejemplo:

```
list ap2
AP2 Statistic       In      Out
-----
Packets:            349      351
Octets:             128488  129412
Prot Rejects:       0
```

dncp Lista las estadísticas de los paquetes del protocolo de control DECnet. Estos campos son los mismos que los descritos bajo el mandato **list ip**. (Consulte la sección “ip” en la página 683.)

Ejemplo:

```
list dncp
DNCP Statistic      In      Out
-----
Packets:            0        0
Octets:             0        0
Prot Rejects:       0        -
```

dn Lista las estadísticas de los paquetes DECnet recibidos y transmitidos a

Supervisión de interfaces PPP (Talk 5)

través de la interfaz PPP. Estos campos son los mismos que los descritos bajo el mandato **list ip**. (Consulte la sección “ip” en la página 683.)

Ejemplo:

```
list dn
DN Statistic      In      Out
-----
Packets:          0        0
Octets:           0        0
Prot Rejects:     0        -
```

osicp Lista las estadísticas para el protocolo de control OSI. Estos campos son los mismos que los descritos bajo el mandato **list ip**. (Consulte la sección “ip” en la página 683.)

Ejemplo:

```
list osicp
OSICP Statistic   In      Out
-----
Packets:          0        0
Octets:           0        0
Prot Rejects:     0        -
```

osi Lista las estadísticas de los paquetes OSI recibidos y transmitidos a través de la interfaz PPP. Estos campos son los mismos que los descritos bajo el mandato **list ip**. (Consulte la sección “ip” en la página 683.)

Ejemplo:

```
list osi
OSI Statistic     In      Out
-----
Packets:          0        0
Octets:           0        0
Prot Rejects:     0        -
```

bvcp Lista las estadísticas del protocolo de control Banyan VINES. Estos campos son los mismos que los descritos bajo el mandato **list ip**. (Consulte la sección “ip” en la página 683.)

Ejemplo:

```
list bvcp
BVCP Statistic    In      Out
-----
Packets:          0        0
Octets:           0        0
Prot Rejects:     0        -
```

vines Lista las estadísticas para los paquetes Banyan VINES recibidos y transmitidos a través de la interfaz PPP. Estos campos son los mismos que los descritos bajo el mandato **list ip**. (Consulte la sección “ip” en la página 683.)

Ejemplo:

```
list vines
Vines Statistic   In      Out
-----
Packets:          10       13
Octets:           320     340
Prot Rejects:     0        -
```

isrcp Lista las estadísticas de los paquetes de protocolo de control APPN ISR. Estos campos son los mismos que los descritos bajo el mandato **list ip**. (Consulte la sección “ip” en la página 683.)

Ejemplo:

```
list isrcp
APPN ISRCP Statistic In      Out
-----
Packets:          3        3
Octets:           12       12
Prot Rejects:     0        -
```

isr Lista las estadísticas de los paquetes APPN ISR recibidos y transmitidos a

Supervisión de interfaces PPP (Talk 5)

través de la interfaz PPP. Estos campos son los mismos que los descritos bajo el mandato **list ip**. (Consulte la sección “ip” en la página 683.)

Ejemplo:

```
list isr
APPN ISR Statistic      In          Out
-----
Packets:                220        219
Octets:                 1266      1157
Prot Rejects:          0          -
```

hprcp Lista las estadísticas de los paquetes del protocolo de control APPN HPR. Estos campos son los mismos que los descritos bajo el mandato **list ip**. (Consulte la sección “ip” en la página 683.)

Ejemplo:

```
list hprcp
APPN HPRCP Statistic   In          Out
-----
Packets:               3           3
Octets:                12          12
Prot Rejects:         0           -
```

hpr Lista las estadísticas de los paquetes APPN HPR recibidos y transmitidos a través de la interfaz PPP. Estos campos son los mismos que los descritos bajo el mandato **list ip**. (Consulte la sección “ip” en la página 683.)

Ejemplo:

```
list hpr
APPN HPR Statistic     In          Out
-----
Packets:               780        715
Octets:               131907    69685
Prot Rejects:         0          -
```

LLC

Utilice el mandato **LLC** para acceder al indicador de supervisión LLC. Los mandatos LLC se entran en este nuevo indicador. Consulte la sección “Mandatos de supervisión LLC” en la página 255 para ver una explicación de cada uno de estos mandatos.

Nota: Este mandato sólo está disponible cuando APPN se incluye en la carga de software.

Sintaxis:

llc

Interfaces Point-to-Point Protocol y el mandato interface de GWCON

El tráfico de la interfaz PPP se transporta por el controlador de dispositivo básico a nivel de enlace de datos. Las estadísticas adicionales que pueden ser útiles al supervisar los enlaces PPP pueden obtenerse a partir de las estadísticas del controlador de dispositivo, que se visualizan utilizando el mandato **interface** en el entorno GWCON. (Para obtener más información sobre el mandato **interface**, consulte la sección “Capítulo 8. El proceso de operación/supervisión (GWCON - Talk 5) y sus mandatos” en la página 117.)

Las estadísticas de esta sección se visualizan cuando se ejecuta el mandato **interface** en el entorno GWCON (talk 5) para las siguientes interfaces utilizadas en configuraciones de punto a punto:

Ejemplo:

Supervisión de interfaces PPP (Talk 5)

+ interface 12

Net	Net'	Interface	Slot-Port	Self-Test Passed	Self-Test Failed	Maintenance Failed
12	12	PPP/0	Slot: 8 Port: 2	2	1	0

Point to Point MAC/data-link on V.35/V.36 interface

Adapter cable: V.35 DTE

V.24 circuit: 105 106 107 108 109
Nicknames: RTS CTS DSR DTR DCD
PUB 41450: CA CB CC CD CF
State: ON ON ON ON ON

Line speed: 64.000 Kbps
Last port reset: 1 hour, 20 minutes, 42 seconds ago

Input frame errors:
CRC error 0 alignment (byte length) 0
missed frame 182 too long (> 2062 bytes) 0
aborted frame 0 DMA/FIFO overrun 0
Output frame counters:
DMA/FIFO underrun errors 0 Output aborts sent 0

Net Número de interfaz asignado por el software durante la configuración inicial.

Net' Número de interfaz básica tal como la ha asignado el software durante la configuración inicial.

Nota: Para las interfaces de circuito de marcación, Net' es diferente de Net. Para interfaces de circuitos de marcación, Net' indica la interfaz base (RDSI o V.25bis) que el circuito de marcación utiliza.

Interface No

Tipo de interfaz y su número de instancia. El tipo de interfaz Point-to-Point es PPP.

Slot El número de ranura de la interfaz a través de la cual se ejecuta PPP.

Port El número de puerto de la interfaz que ejecuta PPP.

Self-Test: Passed

Número total de veces que la interfaz de punto a punto ha pasado su autoprueba.

Self-Test: Failed

Número total de veces que la interfaz de punto a punto ha fallado su autoprueba.

Maintenance: Failed

El número total de anomalías de mantenimiento.

Adapter cable

Tipo de cable adaptador que se ha configurado; por ejemplo, V.35 DTE.

V.24 circuit

Circuitos que se utilizan en el V.24. Nota: El símbolo - - - en la salida de supervisión indica que el valor o el estado es desconocido.

Nicknames

Señales de control. Nota: El símbolo - - - en la salida de supervisión indica que el valor o el estado es desconocido.

PUB 41450

Asignaciones de patillas. Nota: El símbolo - - - en la salida de supervisión indica que el valor o el estado es desconocido.

Supervisión de interfaces PPP (Talk 5)

State Estado de los circuitos V.24 (activado o desactivado). Nota: El símbolo - - - en la salida de supervisión indica que el valor o el estado es desconocido.

Line speed

Velocidad de línea configurada o valor por omisión asumido (si la velocidad de línea está configurada como 0).

Last port reset

Período de tiempo desde que se ha restablecido el puerto.

CRC error

El número de paquetes recibidos que contenían errores de suma de comprobación y como consecuencia de ello se han eliminado.

Alignment (byte length)

El número de paquetes recibidos que no eran un número par de 8 bits de longitud y como consecuencia de ello se han eliminado.

Too long (> 2048 bytes)

El número de paquetes que eran mayores que el tamaño de trama configurado y como resultado se han eliminado.

Aborted frame

El número de paquetes recibidos que se han cancelado anormalmente por el emisor o un error de línea.

DMA/FIFO overrun

El número de veces que la interfaz serie no ha podido enviar datos con la suficiente rapidez a la memoria del almacenamiento intermedio de paquetes del sistema para recibirlos de la red.

Missed frame

Cuando una trama llega al dispositivo y no hay ningún almacenamiento intermedio disponible, el hardware elimina la trama e incrementa el contador de tramas que faltan.

L & F bits not set

En interfaces serie, el hardware establece información de descriptor de entrada para las tramas que llegan. Si el almacenamiento intermedio puede aceptar la trama completa en la llegada, el hardware establece el primer y último bit de la trama, lo que indica que el almacenamiento intermedio ha aceptado toda la trama. Si no se establece alguno de estos bits, se elimina el paquete, se incrementa el contador L & F bits not set y se borra el almacenamiento intermedio para reutilización.

Nota: No es probable que el contador L & F bits not set se vea afectado por el tráfico.

Output Frame Counters:

DMA/FIFO underrun errors

El número de veces que la interfaz serie no ha podido recuperar datos con la suficiente rapidez de la memoria de almacenamiento intermedio de paquetes del sistema para transmitirlos a la red.

Output aborts sent

El número de transmisiones que se han cancelado anormalmente como petición del software de nivel superior.

Se visualizan estadísticas similares a las siguientes para los circuitos de marcación PPP cuando se ejecuta el mandato **interface** en el entorno GWCON:

```

+interface 29
Net Net' Interface           Self-Test Self-Test Maintenance
29 10  PPP/20                Passed    Failed    Failed
Point to Point MAC/data-link on V.25bis Dial Circuit interface

```

Soporte para la reconfiguración dinámica de Point-to-Point Protocol

Esta sección describe la reconfiguración dinámica (DR) en la medida en que afecta a los mandatos Talk 6 y Talk 5.

Delete Interface de CONFIG (Talk 6)

Point-to-Point Protocol (PPP) soporta el mandato **delete interface** de CONFIG (Talk 6) sin ninguna restricción.

Activate Interface de GWCON (Talk 5)

PPP soporta el mandato **activate interface** de GWCON (Talk 5) con las consideraciones siguientes:

- No puede activar un circuito de marcación PPP ni un circuito de marcación de entrada PPP a menos que la red base del circuito de marcación (del circuito de marcación de entrada) ya esté activada.
- No puede activar un circuito de marcación PPP a menos que su red base se haya establecido para RDSI canalizada.
- No puede activar una red Multilink-PPP (MP).
- No puede activar una red PPP que tenga MP habilitado.
- No puede activar una red PPP cuando el tamaño de almacenamiento intermedio global sea inferior a 1500.

Todos los cambios de la configuración de PPP se activan automáticamente excepto los siguientes:

Los mandatos cuyos cambios no se activan con el mandato activate interface de GWCON (Talk 5)
CONFIG, net, enable ccp Nota: No se habilitará la compresión si se trata de la primera red PPP con el CCP habilitado.
CONFIG, net, set lcp options (mru option) Nota: El valor de MRU no se establecerá superior al tamaño de almacenamiento intermedio asignado para el direccionador en el rearranque.

Reset Interface de GWCON (Talk 5)

PPP soporta el mandato **reset interface** de GWCON (Talk 5) con las consideraciones siguientes:

- No puede restablecer una red Multilink-PPP (MP).
- No puede restablecer enlaces PPP cuya configuración original o la configuración deseada sea un enlace MP dedicado.
- No puede restablecer un circuito de marcación PPP si ha cambiado algún parámetro del circuito de marcación que haya configurado en el indicador dial-circuit config>.
- No puede restablecer una interfaz PPP que se esté utilizando para la Restauración de WAN o el Redireccionamiento WAN.

Supervisión de interfaces PPP (Talk 5)

Todos los cambios de la configuración de PPP se activan automáticamente excepto los siguientes:

Mandatos cuyos cambios no se activan por el mandato reset interface de GWCON (Talk 5)
--

CONFIG, net, enable ccp

Nota: No se habilitará la compresión si se trata de la primera red PPP con el CCP habilitado.
--

CONFIG, net, set lcp options (mru option)

Nota: El valor de MRU no se establecerá superior al tamaño de almacenamiento intermedio asignado para la interfaz PPP en el re arranque.

Capítulo 45. Utilización de Multilink PPP Protocol

Este capítulo describe cómo utilizar Multilink PPP Protocol (MP). Incluye las secciones siguientes:

- “Consideraciones acerca de MP” en la página 692
- “MP de múltiples chasis” en la página 693
- “Configuración de una interfaz Multilink PPP” en la página 693

Multilink PPP Protocol le permite aumentar el ancho de banda de:

- Las líneas PPP alquiladas, incluyendo las canalizadas y los circuitos I43x RDSI
- Los circuitos de marcación RDSI de PPP
- Los circuitos de marcación PPP V.25bis
- Los circuitos con túneles PPP de capa 2

El aumento del ancho de banda se consigue mediante la definición de un **enlace virtual** compuesto de múltiples enlaces. El ancho de banda del paquete MP resultante es casi igual a la suma de los anchos de banda de los enlaces individuales. La ventaja es que los grandes paquetes transmitidos a través de un solo enlace ahora pueden dividirse, transmitirse a través de múltiples enlaces y volverse a construir en la estación final de recepción. MP utiliza Bandwidth Allocation Protocol y Bandwidth Allocation Control Protocol para añadir y desactivar dinámicamente circuitos de marcación PPP a un enlace virtual. MP también utiliza el Ancho de banda a petición (BOD) para añadir enlaces de marcación MP “dedicados” a un paquete existente.

Hay dos tipos de enlaces MP: los que están dedicados y los que sólo están habilitados. Un enlace MP dedicado es una interfaz con MP habilitado que está configurada como un enlace con una interfaz MP en particular. Si el enlace intenta unirse a otro paquete MP, o si no se negocia MP, el software termina el enlace. Todos los enlaces PPP excepto las interfaces con túneles de capa 2 pueden configurarse como enlaces MP dedicados. Los enlaces alquilados PPP deben estar configurados como enlaces MP dedicados.

Los circuitos de marcación PPP y los túneles de capa 2 pueden configurarse como MP habilitado. Un enlace con MP habilitado que no está dedicado puede convertirse en un enlace de cualquier paquete MP. Si no se negocia MP, el enlace funciona como una interfaz independiente utilizando los protocolos configurados del enlace.

Puede configurar una interfaz Multilink PPP que conste de múltiples circuitos de marcación PPP como parte del paquete MP.

También hay dos tipos de interfaces MP: las que tienen un enlace dedicado y las que no lo tienen. Una interfaz MP necesita un enlace dedicado en cualquiera de las situaciones siguientes:

- El enlace sólo es para la interfaz MP
- La interfaz MP está configurada para llamadas de salida. El enlace dedicado debe configurarse entonces con el número de teléfono de destino y la identificación del llamador.
- La interfaz MP está configurada para recibir una llamada de entrada en particular. En este caso, el enlace dedicado se configura con el número de teléfono de destino de entrada y la identificación del llamador.
- La interfaz MP necesita realizar la autenticación de salida. En este caso, todos los enlaces utilizan el mismo nombre de autenticación.

Utilización de MP

Las interfaces MP que no tienen un enlace dedicado deben ser interfaces de sólo entrada. Estas interfaces son similares a las de cualquier circuito de marcación.

Bandwidth Allocation Protocol (BAP) y su protocolo de control (BACP) permiten que una interfaz MP aumente y reduzca su ancho de banda añadiendo y desactivando circuitos de marcación. Cuando el algoritmo de utilización de ancho de banda determina que debe añadirse un enlace al paquete, si existe un circuito de marcación PPP disponible y el similar está de acuerdo, se realiza una llamada adicional.

Primero, BAP busca cualquier circuito de marcación PPP dedicado desocupado para la interfaz MP y, después, cualquier circuito de marcación PPP con MP habilitado. Sin embargo, no utilizará un circuito de marcación PPP dedicado de otro circuito MP. El número máximo configurado de enlaces en la interfaz MP no se excederá nunca.

BOD utiliza números de teléfono de circuitos de marcación configurados para realizar llamadas cuando es necesario añadir enlaces de marcación MP dedicados a un paquete existente. Los enlaces se añaden al paquete de uno en uno, si es necesario, durante el período de sondeo. BOD añade primero cualquier enlace serie PPP al paquete y conservará los enlaces serie todo lo que dure el paquete. BOD sólo desactiva enlaces de marcación.

MP soporta las características siguientes:

- BRS
- WRR
- WRS
- Marcación a petición
- DIALs

Sin embargo, WRS, Marcación a petición y DIALs sólo se soportan en paquetes MP que sólo contienen circuitos de marcación.

Consideraciones acerca de MP

Cuando configure un paquete MP, recuerde lo siguiente:

- Mezclar circuitos de marcación con líneas “alquiladas” hace que el software inhabilite BAP en el paquete y que utilice BOD en su lugar. Sólo mezcle circuitos de marcación con circuitos “alquilados” cuando desee utilizar BOD para gestionar el paquete.
- No puede utilizar la Marcación a petición ni WRS para paquetes MP que contengan líneas “alquiladas” PPP o circuitos con túneles de capa 2.
- No puede utilizar DIALs en paquetes que contengan líneas “alquiladas” PPP.
- Todos los dispositivos que se unen a un paquete MP deben tener configurada la velocidad de línea.

Importante:

1. No configure un paquete con soportes con propiedades extremadamente diferentes. Por ejemplo, la configuración de un paquete que contenga un enlace HSSI y un enlace V.25bis no es una utilización eficaz de un paquete. El enlace mayor no debe tener más de 4 veces la capacidad del enlace más pequeño. Si las velocidades de los enlaces de un paquete MP difieren mucho, puede que necesite añadir almacenamientos intermedios de recepción en el enlace más rápido.

2. Cuando empaquete canales B RDSI con tipos de soporte más lentos, puede que necesite aumentar el número de almacenamientos intermedios RDSI. El empaquetamiento de canales B RDSI con enlaces más lentos no está recomendado para el RDSI primario.

MP de múltiples chasis

Un paquete MP con un Túnel de capa 2 que contiene un grupo de búsqueda de teléfonos que se fragmenta entre múltiples Servidores de acceso a la Red físicos, se conoce como *MP de múltiples chasis*. MP de múltiples chasis utiliza la función de túnel basada en el usuario o rhelm (consulte la sección “Utilización de autenticación local o remota” de la publicación *Utilización y configuración de las características*) para establecer el destino de punto final MP. Consulte la sección “Utilización de Layer 2 Tunneling Protocol (L2TP)” de la publicación *Utilización y configuración de las características* para obtener más información acerca de L2TP.

Configuración de una interfaz Multilink PPP

La configuración de una interfaz MP depende del tipo de interfaz utilizada en el paquete MP. Las secciones siguientes contienen ejemplos de varias configuraciones.

Después de configurar la interfaz MP, puede configurar el ancho de banda a petición (BOD). El ejemplo siguiente configura BOD en la interfaz MP 17 existente:

```
Config> net 17
MP config: 17> enable bod
Enable BAP? [N]

MP config: 17> set bandwidth-on-demand parameters
Add bandwidth % [90]:
Drop bandwidth % [70]:
Bandwidth test interval (sec) [15]

MP config: 17>
```

Configuración de MP en circuitos de marcación PPP

Esta sección muestra cómo configurar una interfaz Multilink PPP utilizando un ejemplo que configura Multilink PPP con dos circuitos de marcación RDSI.

1. Añada los dos circuitos de marcación y la interfaz multilink PPP.

```
*t 6

Config>add dev dial-circuit
Adding device as interface 7
Defaulting Data-link protocol to PPP
Use "net 7" command to configure circuit parameters
Config>add dev dial-circuit
Adding device as interface 8
Defaulting Data-link protocol to PPP
Use "net 8" command to configure circuit parameters
Config>add dev multilink-ppp
Enter the number of multilink PPP interfaces [1]?
Adding device as interface 9
Defaulting Data-link protocol to PPP
Use "net intf" command to configure circuit parameters
Config>
```

2. Configure cada circuito de marcación PPP. (Consulte la sección “Capítulo 54. Configuración y supervisión de circuitos de marcación” en la página 797.) En este ejemplo, se establecen el destino, la dirección de la llamada y los LID para uno de los circuitos de marcación.

Utilización de MP

```
Config>net 7
Circuit configuration
Circuit config: 7>set dest out
Circuit config: 7>set calls outbound
Circuit config: 7>set net 6
Circuit config: 7>
```

3. Habilite MP en cada circuito de marcación que se ha de utilizar para MP de la manera siguiente:

```
Circuit config: 7>encapsulator
Point-to-Point user configuration
PPP 7 Config>enable mp
```

```
Enabled as a Multilink PPP Link,
Use as a dedicated Multilink PPP link? [No]: yes
Multilink PPP net for this Multilink PPP link [1]? 9
NOTE: PPP configuration will be obtained from the Multilink PPP
net. It is NOT necessary to configure PPP for this net!
```

Nota: No puede configurar los parámetros PPP para enlaces dedicados desde este indicador. Los enlaces dedicados utilizan la configuración PPP de la interfaz MP existente.

Si se responde “Yes” a la pregunta “Use as a dedicated Multilink PPP link?” el enlace se convierte en dedicado para la interfaz Multilink PPP especificada (9 en este ejemplo). En este caso, el enlace **debe** utilizarse para un paquete MP y **debe** unirse a la interfaz MP especificada. El enlace no puede utilizarse como un circuito de marcación PPP normal.

Si se responde “No” a “Use as a dedicated Multilink PPP link?” se permitirá que este circuito de marcación PPP se una a cualquier interfaz MP. Como mínimo un circuito de marcación PPP **debe** ser un enlace dedicado para la interfaz MP de salida.

Un circuito de marcación PPP dedicado obtiene todos los parámetros PPP (opciones LCP, autenticación y otros) de su interfaz MP. Los circuitos de marcación PPP con MP habilitado que se unen al mismo paquete MP **deben** negociar los mismos parámetros LCP y nombre de autenticación.

4. Configure la interfaz MP. Los protocolos, BAP, BRS, la restauración de WAN, el redireccionamiento de WAN y la marcación a petición se ejecutan en la interfaz MP y no en los circuitos de marcación PPP.

Configuración de MP en enlaces serie PPP

Para configurar MP en un enlace serie PPP, habilite MP en la interfaz utilizando el mandato **net**. El enlace obtiene su configuración PPP de la red MP.

Ejemplo:

```
Config> net 1
PPP 1 Config> enable MP
```

```
Multilink PPP net for this Multilink PPP link [1]? 8
NOTE: PPP configuration will be obtained from the Multilink PPP
net. It is NOT necessary to configure PPP for this net!
PPP 1 Config>
```

Configuración de MP en redes con túneles de capa 2

Para configurar MP en una red L2TP, se habilita MP a través del encapsulador L2TP. Después, deben configurarse los mismos parámetros de negociación PPP (consulte la sección “Configuring L2TP” en la publicación *Utilización y configuración de las características*) para obtener información acerca de todas las redes que se unen en un solo paquete.

Ejemplo:

```
Config> feature layer-2-tunneling
Layer-2-Tunneling Config> encapsulator
PPP-L2TP Config> enable mp
```

NOTE: It IS necessary to configure PPP for this net! PPP negotiation parameters must be configured the same for all nets wishing to join the same Multilink PPP bundle.
PPP-L2TP Config>

Configuración de MP de múltiples chasis

Para configurar MP para MP de múltiples chasis, configure la característica DIALs para MP de múltiples chasis. El software le solicita el discriminador de punto final que se ha de utilizar.

Ejemplo:

```
Config> feature DIALs
DIALs Config> set multi-chassis-mp
Enter Endpoint Discriminator to use from stacked group (0 for box S/N): 2345
DIALs Config>
```

El ejemplo siguiente muestra MP de múltiples chasis cuando los puertos RTR-2 y RTR-3 están en un grupo de búsqueda.

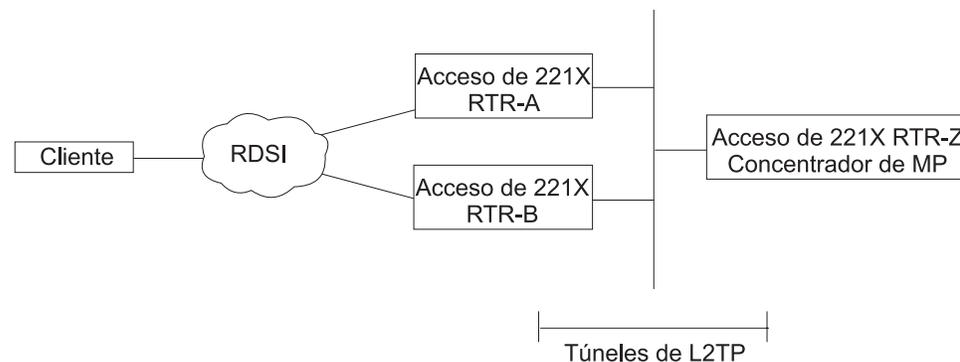


Figura 48. MP de múltiples chasis

Puesto que hay una relación de muchos a muchos entre los direccionadores de acceso y los concentradores MP, deben mantenerse todos los direccionadores de acceso (RTR-A, RTR-B) en un dominio de administración separado de los direccionadores concentradores MP (RTR-Z). Esto se aplica si desea utilizar la autenticación remota (es decir, RADIUS), necesitará dos servidores RADIUS, uno para los direccionadores de acceso y otro para los concentradores MP. Si utiliza una lista local, ya utiliza dominios de administración separados.

En este escenario, puede elegir la función de túnel basándose en el nombre de usuario PPP o el nombre de "rhelm". Es menos riguroso utilizar el túnel basado en rhelm. La idea es configurar un perfil de túnel para RTR-Z en RTR-A y RTR-B. No se necesitan usuarios PPP adicionales en estos direccionadores. RTR-Z necesitaría 2 perfiles de túnel: uno para RTR-A y otro para RTR-B y un nombre de usuario PPP (con el formato <nombreusuario>@RTRZ) para cada usuario previsto. Todos los circuitos de marcación de entrada se configuran en los direccionadores de "acceso". Los "concentradores MP" tendrían dispositivos de túnel de capa 2 y dispositivos Multilink PPP.

Utilización de MP

Ahora ha configurado estadísticamente un MP de múltiples chasis. Esto significa que un nombre de usuario PPP en particular siempre terminará MP en un direccionador preconfigurado y no será necesario soportar un protocolo adicional que busque dinámicamente las cabeceras y túneles del paquete MP cuando sea necesario. Esta implementación de la red también ayudará a evitar las idiosincrasias de la negociación PPP de clientes cuando se utilicen tipos de soporte diferentes para cada enlace de un paquete (por ejemplo, túnel en un enlace y no en el otro). Por ejemplo, los clientes DIALs no pueden volver a negociar LCP en ningún momento. Tampoco, los clientes Microsoft DUN soportan totalmente la renegociación LCP.

Interposición de paquetes en Multilink PPP

La interposición de paquetes en Multilink PPP proporciona soporte para el servicio integrado que permite interponer múltiples clases de datos durante la transmisión. Esto minimizará los retardos de extremo a extremo para los flujos multimedia en tiempo real.

La interposición de paquetes se puede habilitar o inhabilitar. Para obtener información de configuración, consulte "Mandatos de configuración MP para interfaces Multilink PPP" en la página 697.

Capítulo 46. Configuración y supervisión de Multilink PPP Protocol (MP)

Este capítulo describe cómo configurar interfaces Multilink PPP específicas en un dispositivo. Incluye:

- “Acceso al indicador de configuración MP”
- “Mandatos de configuración MP para interfaces Multilink PPP”
- “Supervisión del estado de interfaces MP” en la página 701
- “Acceso a los mandatos de supervisión MP” en la página 701
- “Mandatos de supervisión Multilink PPP Protocol” en la página 701

Acceso al indicador de configuración MP

Para acceder al indicador MP `config`:

1. Entre **talk 6** en el indicador `*`.
2. Entre **net n**, donde *n* es el número del circuito de marcación o la interfaz MP que ha habilitado para utilizar MP.

Nota: Ahora, está configurando la interfaz Multilink PPP y no el circuito de marcación PPP que forma parte del paquete MP.

Mandatos de configuración MP para interfaces Multilink PPP

La Tabla 83 lista los mandatos disponibles en el indicador MP `config`.

Tabla 83. Mandatos de configuración MP

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página 10.
Disable	Inhabilita la interposición y la negociación del ancho de banda a petición.
Enable	Habilita la interposición y la negociación del ancho de banda a petición.
Encapsulator	Le coloca en el indicador PPP <code>config</code> para que pueda cambiar la configuración del protocolo de enlace de datos.
List	Visualiza los parámetros de configuración de la interfaz MP.
Set	Configura la interfaz MP para el tráfico de entrada o de salida. También le permite establecer el tiempo de espera excedido de desocupado y otros parámetros MP y BAP.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página 11.

Disable

Utilice el mandato **disable** para inhabilitar la negociación del ancho de banda a petición (BOD) e inhabilitar la interposición. La inhabilitación de BOD impide que el enlace asigne ancho de banda adicional cuando es necesario. La inhabilitación de la interposición inhabilita el servicio integrado que permite interponer múltiples clases de datos durante la transmisión.

Sintaxis:

disable bod
interleaving

Configuración de MP

Enable

Utilice el mandato **enable** para habilitar la negociación de BOD y para habilitar la interposición. La habilitación de BOD permite que el enlace asigne ancho de banda adicional cuando es necesario. La habilitación de la interposición permite interponer múltiples clases de datos durante la transmisión.

Sintaxis:

enable

bod

interleaving

```
MP config: 0>enable interleaving
Interleaving Enabled. New MaxFrag = 200, new MinFrag = 128
```

```
NOTE: Interleavable traffic will not be compressed and/or encrypted
even if these functions are enabled for this interface!!!!
```

Encapsulator

Utilice el mandato **encapsulator** para acceder a la configuración de la capa de enlace PPP para la interfaz Multilink PPP.

Sintaxis:

encapsulator

Ejemplo:

```
encapsulator
Point-to-Point user configuration
PPP config>
```

List

Utilice el mandato **list** para visualizar la configuración MP actual.

Sintaxis:

list

Ejemplo:

```
list
Idle timer = 0 (fixed circuit)
Outbound calls = allowed
Dialout MP Link net = 7
Max fragment size = 750
Min fragment size = 375
Maximum number of active links = 2
Links associated with this MP bundle:
net number 7
net number 8
Interleaving =Disabled

BAP enabled
Add bandwidth percentage = 90
Drop bandwidth percentage = 70
Bandwidth test interval (sec) = 15
```

Idle timer

El valor del temporizador de desocupado para este circuito en segundos.

El valor 0 indica un circuito fijo. Un valor distinto de cero configura un circuito MP de marcación a petición que se desactivará cuando el circuito esté desocupado durante el número de segundos especificado. El circuito se vuelve a activar cuando se reanuda el tráfico de red.

Outbound calls

Especifica si la interfaz está configurada para iniciar llamadas de salida. Si la interfaz no puede iniciar llamadas de salida, no se visualiza esta línea.

Inbound calls

Especifica si la interfaz está configurada para iniciar llamadas de entrada. Si la interfaz no puede aceptar llamadas de entrada, esta línea no se visualiza.

Max fragment size

Especifica el número máximo de bytes de datos que puede contener un paquete antes de que se fragmente para enviarse a través de los enlaces MP.

Min fragment size

Este es el tamaño mínimo de los fragmentos (en bytes) que el software crea cuando un paquete excede del **Max fragment size**.

Maximum number of active links

Especifica el número máximo de enlaces configurados en el enlace virtual MP (conocido también como **paquete**).

Links associated with this MP bundle

Visualiza los enlaces dedicados a esta interfaz MP.

Interleaving

Especifica si se está utilizando o no la interposición de paquetes. Esta característica necesita una configuración adicional de la Capa de clasificación (p.ej., BRS, DiffServ)

BAP enabled

Especifica si BAP está habilitado en esta interfaz.

Add bandwidth percentage

La cantidad de utilización de ancho de banda a la que el software intentará añadir un nuevo enlace si BAP está habilitado.

Drop bandwidth percentage

La cantidad de utilización de ancho de banda a la que el software eliminará un enlace del paquete MP si BAP está habilitado.

Bandwidth test interval

El tiempo, en segundos, después del cual el software comprobará la utilización de ancho de banda para determinar si se ha de añadir o desactivar un enlace del paquete.

Set

Utilice el mandato **set** para configurar:

- La interfaz MP para llamadas de entrada o de salida
- El tiempo de espera excedido de desocupado
- Los parámetros MP
- Los parámetros BAP

Sintaxis:

```
set                bd parameters
                   calls
                   idle
                   mp parameters
```

Configuración de MP

bod parameters

Le solicita que especifique los porcentajes de ancho de banda para añadir y eliminar de BOD y el intervalo de prueba de BOD.

Ejemplo:

```
set bod parameters
Add bandwidth % [90]? 80
Drop bandwidth % [70]? 50
Bandwidth test interval (sec) [15]? 25
```

Add bandwidth %

La cantidad de utilización de ancho de banda a la que el software intentará añadir un nuevo enlace.

Valores válidos: De 1 a 99

Valor por omisión: 90

Drop bandwidth %

La cantidad de utilización de ancho de banda a la que el software eliminará un enlace del paquete MP.

Valores válidos: De 1 a 99

Valor por omisión: 70

Bandwidth test interval (sec)

El tiempo, en segundos, después del cual el software comprobará la utilización de ancho de banda para determinar si se ha de añadir o desactivar un enlace del paquete.

Valores válidos: De 10 a 200 segundos

Valor por omisión: 15

calls Especifica si esta interfaz MP iniciará llamadas de salida, sólo aceptará llamadas de salida o participará en ambos tipos de llamada.

Valores válidos: inbound, outbound o both

Valor por omisión: inbound

Nota: Si especifica outbound o both, el software pedirá el número de red del enlace MP dedicado que establecerá la primera llamada.

Ejemplo:

```
set calls outbound
Dialout MP link net for this MP net []? 4
```

idle Especifica el período de tiempo en segundos que una interfaz puede no tener tráfico de protocolo en el que la interfaz MP finalizará llamadas en todos los enlaces.

Valores válidos: De 0 a 65535

Valor por omisión: 0

mp parameters

Le solicita que entre los tamaños máximo y mínimo de fragmento y el número máximo de enlaces activos.

Ejemplo:

```
set mp parameters
Max frag size [750]? 675
Min frag size [375]? 300
Max number of active links [2]? 4
```

Max frag size

Especifica el mayor número de bytes de datos que puede contener un paquete antes de que se fragmente para enviarse a través de enlaces MP.

Valores válidos: De 100 a 3 000

Valor por omisión: 750

Min frag size

Este es el tamaño mínimo de los fragmentos (en bytes) que el software crea cuando un paquete excede del **Max fragment size**.

Valores válidos: De 100 a 3 000

Valor por omisión: 375

Max number of active links

Especifica el número máximo de enlaces configurados en el enlace virtual MP (conocido también como **paquete**).

Valores válidos: De 1 a 64

Valor por omisión: 2

Supervisión del estado de interfaces MP

Para determinar el estado de todas las interfaces MP del dispositivo, utilice el mandato **configuration** en **talk 5** (consulte la sección "Configuration" en la página 120).

Acceso a los mandatos de supervisión MP

Para acceder a los mandatos de supervisión MP:

1. Entre **talk 5** en el indicador *.
2. Entre **net n**, donde **n** es el número de la interfaz MP que se ha creado en talk 6 utilizando el mandato **add device multilink-ppp**.

Mandatos de supervisión Multilink PPP Protocol

La Tabla 84 muestra los mandatos de supervisión disponibles para una interfaz MP.

Tabla 84. Mandatos de supervisión MP

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado "Cómo obtener ayuda" en la página 10.
List	Visualiza las estadísticas de BAP, BACP, BOD y MP, los errores y otra información.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página 11.

List

Utilice el mandato **list** para visualizar la información acerca de la interfaz MP incluyendo las estadísticas de asignación de ancho de banda.

Sintaxis:

Supervisión de MP

```
list
      bacp
      bap
      control bacp
      control bod
      control mp
      mp
```

Nota: Los ejemplos que siguen suponen que la interfaz MP de este dispositivo es la red número 6.

bacp El mandato **list bacp** lista las estadísticas para los paquetes de control de asignación de ancho de banda que se han enviado o recibido en este circuito MP.

Ejemplo:

```
PPP 6> list bacp
```

BACP Statistic	In	Out
-----	--	---
Packets:	6	8
Octets:	60	80
Rejects:	0	-

bap El mandato **list bap** lista las estadísticas de los paquetes de protocolo de asignación de ancho de banda que se han enviado o recibido en este circuito MP.

Ejemplo:

```
PPP 6> list bap
```

BAP Statistic	In	Out
-----	--	---
Packets:	3	3
Octets:	22	37
Call Requests:	1	0
Call Response(ACK):	0	1
Call Resp(NK & FLLNK):	0	0
Call Response(Rej):	0	0
Callback Requests:	0	0
Callback Response(ACK):	0	0
Clbck Resp(NK & FLLNK):	0	0
Callback Response(Rej):	0	0
Drop Requests:	0	1
Drop Response(ACK):	1	0
Drop Resp(NK & FLLNK):	0	0
Drop Response(Rej):	0	0
Call Status(Success):	1	0
Call Status(Fail):	0	0

Hay cuatro respuestas diferentes a la petición de un similar: ACK, NAK, FULL-NAK y REJECT.

ACK Indica que se ha otorgado la petición del similar.

NAK (NK)

Indica que la petición del similar está soportada pero no se desea en este momento. Inténtelo de nuevo más adelante.

FULL-NAK (FLLNK)

Indica que la petición del similar está soportada pero debido a una condición de un recurso, no puede otorgarse en este momento. La petición no debe enviarse de nuevo hasta que cambie el ancho de banda total en el paquete MP.

REJECT (REJ)

Indica que la petición no está soportada.

control bacp

El mandato **list control bacp** lista el estado actual de la máquina de estado BACP en PPP. La información de estado es idéntica a la producida para todos los protocolos de control PPP. También se lista la información acerca del similar favorito. El similar favorito se utiliza para aliviar las colisiones de paquetes BAP (cuando ambos extremos inician peticiones simultáneamente). Durante las negociaciones de BACP, cada extremo envía un número mágico y el que tiene el número mágico menor es el similar favorito y debe tener prioridad en caso de colisión. Normalmente, el iniciador de la llamada elegirá un **número mágico** de X'1' y el receptor de la llamada elegirá un número mágico de X'FFFFFFFF' estableciendo el iniciador de la llamada como similar favorito.

```
PPP 6> list control bacp
```

```
BACP State:                Open
BACP Option                Local                Remote
-----
Magic Number:             FFFFFFFF                1
Favorite Peer:            NO                YES
```

control bod

El mandato **list control bod** lista el estado actual de ancho de banda a petición (BOD). Esta información incluye el estado BAP, los parámetros de ancho de banda a petición configurados para añadir y reducir el ancho de banda, el ancho de banda actual y la información del último sondeo de ancho de banda.

Los estados BAP válidos son:

Closed

BACP no está abierto – BAP no está habilitado o el similar no lo soporta.

Ready BACP está abierto y no hay ninguna petición pendiente que se esté procesando.

Call Req Sent

Hay una petición de llamada pendiente que se ha enviado desde la máquina local.

Callback Req Sent

Hay una petición de llamada de retorno pendiente que se ha enviado localmente.

Call Placed

Como resultado de una petición BAP para añadir ancho de banda, se ha realizado una llamada.

Retry Status Sent

La llamada de salida no ha podido unirse al paquete MP, se ha enviado un estado de reintento.

No Retry Status Sent

La llamada de salida ha sido satisfactoria o ha agotado todos los reintentos, se ha enviado un estado de sin reintento.

Drop Req Sent

Hay una petición de desactivación pendiente que se ha enviado localmente.

Supervisión de MP

Los parámetros de ancho de banda a petición configurados incluyen porcentaje de adición, porcentaje de desactivación, número máximo de enlaces activos en el paquete MP y el intervalo de sondeo de ancho de banda.

Se iniciará una petición BAP para añadir un enlace al paquete si se cumplen las dos condiciones siguientes:

- El número actual de enlaces activos es inferior al número máximo configurado de enlaces.
- La utilización de ancho de banda en todos los enlaces del paquete MP es mayor que el porcentaje de adición del ancho de banda total disponible para el paquete MP.

Se iniciará una petición BAP para desactivar un enlace de PM si se cumplen las dos condiciones siguientes:

- El número de enlaces activos es mayor que uno.
- La utilización de ancho de banda en todos los enlaces del paquete MP es inferior al porcentaje de desactivación del ancho de banda total disponible para el paquete MP para el número de enlaces menos uno.

El ancho de banda sólo se puede sondear cuando BAP está en el estado preparado. La información listada del sondeo anterior le ofrecerá una idea de la utilización de ancho de banda en el paquete MP.

Se visualizan estos dos conjuntos de información cuando se puede iniciar una desactivación:

- Utilización de ancho de banda en todo el paquete
- Utilización de ancho de banda en el número de enlaces menos uno

Para evitar la eliminación, se utiliza el segundo conjunto de información s cuando se determina si se ha de desactivar un enlace.

Ejemplo:

```
PPP 11>list control bod
```

```
BOD :                               Disabled
BAP :                               Disabled
Bandwidth test interval (sec):      15
Add bandwidth percentage:           90
Drop percentage (links-1):          70
  Max # active links in MP bundle:   2
Time since last Bandwidth check (sec): 19
Currently:
  # active links in MP bundle:        0
  Total MP bandwidth (Bytes/sec):     0
Last Bandwidth Check:
  # active links in MP bundle:        0
  Avg Inbound bandwidth util (%):     0
  Avg Outbound bandwidth util (%):    0
```

control mp

El mandato **list control mp** lista el estado actual del circuito MP incluyendo el número de enlaces activos y el ancho de banda, el número máximo de enlaces configurado y las estadísticas para el número de paquetes desactivados. Los paquetes MP desactivados se clasifican en cuatro categorías:

- M** El paquete se desactiva porque no se ha recibido un número de secuencia y es menor que el número mínimo de secuencia del último número de secuencia recibido en todos los enlaces.

Timeout

El paquete se desactiva porque no se ha recibido un número de secuencia durante un período de tiempo de espera excedido.

Q depth

El paquete se desactiva porque se ha excedido la profundidad máxima de cola.

Seq order

El paquete se ha desactivado porque no se esperaba el número de secuencia recibido. Esto se produce cuando MP recibe un paquete retrasado que ya se había declarado perdido.

Si se desactiva un paquete en la capa de red, puede ser un paquete M, Timeout o Q depth. Estos contadores se incrementan adecuadamente cuando se desactiva un paquete.

Interleaving

Especifica si se está utilizando o no la interposición de paquetes.

```
PPP 1> list control mp
Current # active links in MP bundle:      2
Max # active links in MP bundle:        2
Total MP bandwidth (Bytes/sec):         512000
Dropped Frags (lost packets):           0
Dropped Frags (timeout or receive overflow): 0
Dropped Frags (sequence not expected):   0
Interleaving:                           Disabled

PPP 1>
```

mp

El mandato **list mp** lista las estadísticas para los paquetes que se han enviado o recibido en este circuito MP. Esta cuenta de paquetes representa el número de paquetes que se ha clasificado como datos que se pueden interponer y se han transmitido fuera de la interfaz MP. El número de bytes visualizado para los paquete predescomprimidos si se ha negociado la compresión para el paquete multilink PPP.

```
PPP 6> list mp

MP Statistic           In           Out
-----
Bytes (Compressed):    61230        60259
Interleaved packet count: NA 0 has been added.
```

Supervisión de MP

Capítulo 47. Configuración y supervisión de SDLC Relay

Este capítulo incluye una visión general de la función Synchronous Data Link Control (SDLC) Relay y describe sus mandatos de configuración y operativos.

Para obtener más información de cuándo utilizar DLSw SDLC en contraposición a SDLC Relay, consulte la sección “Relación con la función SDLC Relay” del capítulo “Utilización de DLSw” de la publicación *Consulta de configuración y supervisión de protocolos Volumen 1*.

El capítulo incluye las secciones siguientes:

- “Visión general de SDLC Relay”
- “Procedimiento de configuración básica” en la página 709
- “Reconfiguración dinámica” en la página 709
- “Acceso al entorno de supervisión SDLC Relay” en la página 717
- “Mandatos de supervisión SDLC Relay” en la página 718
- “Interfaces SDLC Relay y el mandato interface de GWCON” en la página 720
- “Soporte para la reconfiguración dinámica de SDLC Relay” en la página 720

Visión general de SDLC Relay

SDLC Relay es una función que transporta paquetes SDLC encapsulados en IP a través de una conexión IP. Las conexiones SDLC constan de un punto final primario (sondeo) y un punto final secundario (sondeado). Son de punto a punto (un dispositivo primario y un dispositivo secundario) o multipunto (un dispositivo primario y varios dispositivos secundarios). SDLC Relay mantiene este diseño, excepto en que los direccionadores reenvían las tramas entre los dispositivos SDLC primarios y secundarios.

La Figura 49 en la página 708 muestra un ejemplo de la configuración de SDLC Relay con el dispositivo SDLC primario conectado a dos unidades de control SDLC secundarias.

Configuración y supervisión de SDLC Relay

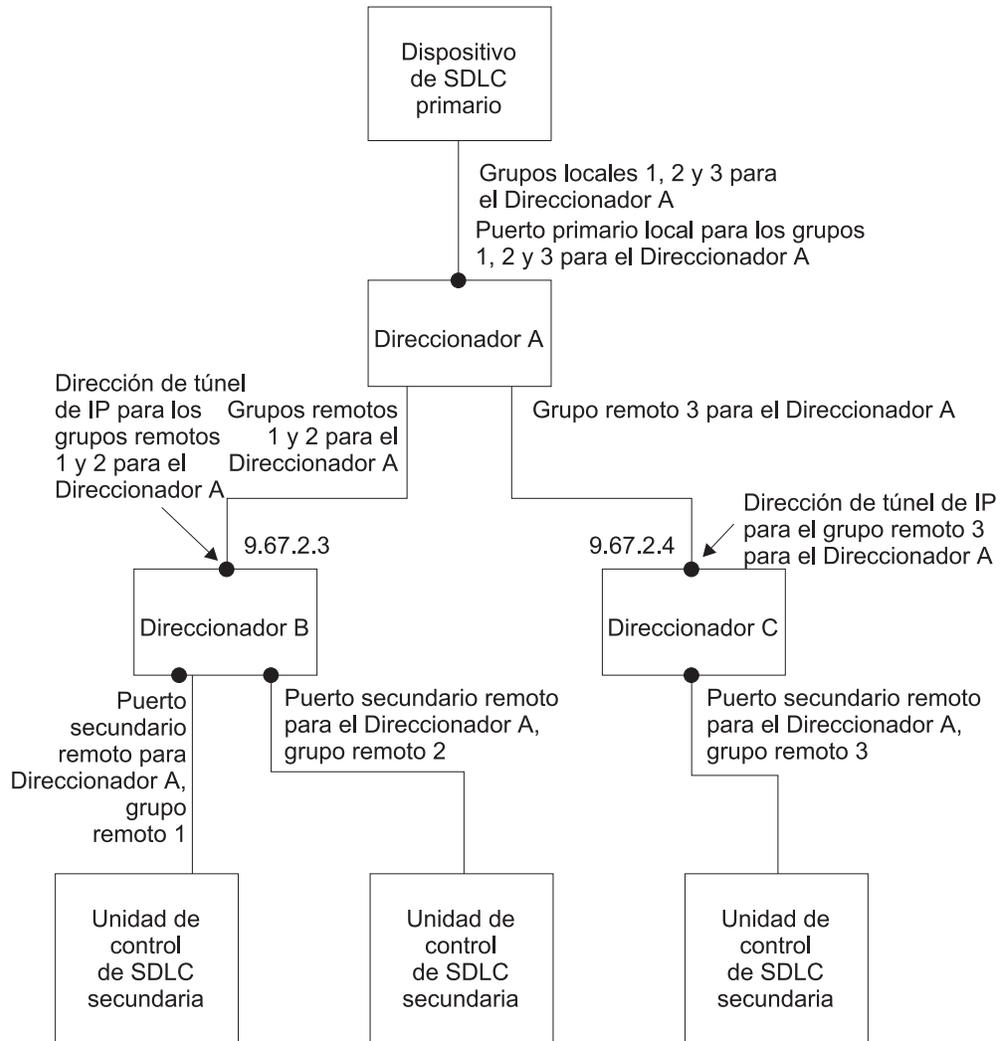


Figura 49. Ejemplo de una configuración SDLC Relay

Tal como se muestra, los dispositivos SDLC primario y secundarios están conectados localmente a un direccionador. Los direccionadores se comunican a través de una conexión IP o túnel y sirven como conducto entre los puntos finales SDLC. Durante la configuración, puede definir las conexiones con los direccionadores como grupos virtuales. También puede asignar números arbitrarios a estos grupos para identificarlos en el direccionador. Un grupo local incluye un puerto local, que es una interfaz local de un direccionador. Cada grupo local tiene un grupo remoto correspondiente que consta de un puerto remoto, que es la interfaz del direccionador remoto, y la dirección de un túnel IP que conecta el direccionador local con el direccionador remoto. El direccionador remoto es similar al direccionador local. Por ejemplo, el Direccionador B y el Direccionador C son direccionadores remotos para el Direccionador A. La dirección IP del túnel debe ser la dirección IP interna del direccionador remoto. Consulte el mandato `set internal-IP-address` de la publicación *Consulta de configuración y supervisión de protocolos Volumen 2* para obtener más información.

También se identifica cada puerto como primario o secundario, dependiendo del punto final de la conexión. En cada grupo, un puerto es primario y otro es secundario. Aunque los grupos del ejemplo tengan el mismo número para el grupo local y el grupo remoto correspondiente, esta coincidencia no es necesaria. Por

Configuración y supervisión de SDLC Relay

ejemplo, para el Direccionador A, el grupo local 2 incluye el puerto primario local para el grupo local 2. El grupo remoto correspondiente también tiene el número 2, pero se hubiese podido identificar por otro número.

Las unidades de control SDLC secundarias conectadas al Direccionador B de este ejemplo, no están conectadas a la misma línea. Se trata de un ejemplo de conexión multipunto virtual. Si las unidades de control SDLC están directamente conectadas a la misma línea, se considera una conexión física. En una red, puede haber conexiones físicas y virtuales.

En una red multipunto, los dispositivos secundarios se identifican por direcciones de estación de un byte o de dos bytes. Todos los direccionadores SDLC Relay de una red SDLC deben utilizar el mismo número de bytes de dirección, todos un byte o todos dos bytes. Los direccionadores identifican las unidades de control SDLC secundarias dinámicamente. Basándose en este reconocimiento, los direccionadores pueden transmitir tramas para un dispositivo en particular a ese dispositivo. Las tramas de difusión continúan siendo difundidas desde el dispositivo emisor a todos los demás dispositivos de la red.

Sólo está soportada la modalidad de transmisión semi-dúplex. Esto significa que deben emitirse peticiones de emisión (RTS) antes de cada transmisión. Preparado para transmitir (CTS) no permanece activado permanentemente.

Procedimiento de configuración básica

Esta sección indica los pasos de configuración mínima que es necesaria para activar y ejecutar el protocolo SDLC Relay. Para ver una explicación más profunda de los parámetros, consulte la sección "Visión general de SDLC Relay" en la página 707 y las descripciones de los mandatos de configuración.

- *Añada un grupo local.* Debe configurar el grupo local utilizando el mandato **add group**.
- *Añada un puerto local.* Esto identifica la interfaz que está utilizando para el puerto local. También asegura que no haya ninguna dirección IP configurada para la interfaz que selecciona. Utilice el mandato **add local-port**.
- *Añada un puerto remoto.* Esto identifica el puerto conectado directamente a la parte remota de la línea serie. Utilice el mandato **add remote-port**.

Reconfiguración dinámica

Puede utilizar los mandatos **reset númerointerfaz** y **activate númerointerfaz** de Talk 5 para activar todos los parámetros de SDLC Relay que haya configurado en una interfaz utilizando Talk 6. Alternativamente, puede reiniciar o volver a cargar el direccionador para que los nuevos cambios en la configuración surtan efecto.

Acceso al entorno de configuración SDLC Relay

Para acceder al entorno de configuración SDLC relay (SRLY):

1. En el indicador Config>, entre **set data-link srlly**.
2. Entre el número de interfaz.
3. Para configurar la interfaz SRLY, entre el mandato **network númerointerfaz**. Se visualiza el indicador SRLY *númerointerfaz* Config> cuando se entra **network númerointerfaz**:

```
Config>network 2
SDLC Relay interface user configuration
SRLY 1 Config>
```

Configuración y supervisión de SDLC Relay

- Para configurar los parámetros del protocolo SRLY, entre el mandato **protocol sdlc**. Se visualiza el indicador SDLC Relay config> cuando se entra **protocol sdlc**:

```
Config>protocol sdlc
SDLC Relay protocol user configuration
SDLC Relay config>
```

Mandatos de configuración SDLC Relay

Esta sección resume los mandatos de configuración SDLC Relay. En este capítulo se documentan los parámetros **network** y **protocol** para SDLC Relay.

Los mandatos de configuración SDLC Relay le permiten especificar los parámetros de direccionador para las interfaces que transmiten tramas SDLC Relay. La Tabla 85 muestra los mandatos para **network sdlc** y **protocol sdlc**.

Tabla 85. Resumen de los mandatos de configuración SDLC Relay

Mandato	Red SRLY	Protocolo SDLC	Función
? (Ayuda)	sí	sí	Lista todos los mandatos de configuración SDLC Relay o lista las opciones asociadas con mandatos específicos.
Add		sí	Añade grupos, puertos locales y puertos remotos.
Delete		sí	Suprime grupos y puertos.
Disable		sí	Inhabilita grupos y puertos.
Enable		sí	Habilita grupos y puertos.
List	sí	sí	Visualiza las configuraciones de todo SDLC Relay y las específicas de grupos.
Set	sí		Establece los parámetros de enlace y los parámetros de estación remota.
Exit	sí	sí	Salte del entorno de configuración de SDLC Relay y vuelve al entorno CONFIG.

Add

Utilice el mandato **add** para añadir grupos locales, puertos locales y puertos remotos.

Sintaxis:

```
add group númerogrupo-local tipo-grupo
      nombre-grupo-local
      local-port
      remote-port
```

group Define un grupo local. Un grupo local se identifica por un número y un nombre.

Ejemplo: add group

```
Local group number: [1]?
Local group name []? CHICAGO-TO-MIAMI
(P)oint-to-Point or (M)ultipoint: [P]?
```

número-grupo-local

El número de grupo que está designando para identificar el grupo local.

nombre-grupo-local

Se trata del nombre de este grupo local. Puede utilizar un máximo

Configuración y supervisión de SDLC Relay

de 32 caracteres ASCII para nombrar el grupo local. Si no proporciona un nombre, se utiliza el nombre por omisión de LOCAL-GROUP-*n*, donde *n* es el número de grupo local.

Group-type

Los tipos de grupos son de punto a punto o multipunto.

local-port

Identifica la interfaz que está utilizando para el puerto local.

Ejemplo: add local-port

```
Local group number: [1]?  
Interface number: [0]? 3  
(P)rimary or (S)econdary: [S]? p
```

Local group number

El número de grupo local para el puerto.

Network or interface number

El número de red o interfaz del direccionador que designa el puerto local.

Primary or Secondary

Designa el tipo de puerto, primario (P) o secundario (S). El valor por omisión es secundario.

remote-port

Identifica el puerto directamente conectado a la línea serie del direccionador remoto.

Ejemplo: add remote-port

```
Local group number: [1]?  
IP address of remote router: [0.0.0.0]? 9.67.2.3  
Is the remote's upper group number limit 255 (current) or 15 (migration): [255]?  
Remote router group number: [1]?  
Does the connection use 2-byte station addressing: [Y]?  
(P)rimary or (S)econdary: [S]? s
```

Group number

El número de grupo local para el puerto.

IP address of remote router

La dirección IP interna del direccionador remoto. Identifica el túnel IP que conecta el direccionador con el direccionador remoto.

Upper group number limit

Nivel de soporte del direccionador remoto, definido por el límite superior de los números de grupo que puede utilizar. El valor por omisión es el actual, que es un límite de 255 y un rango de 1 a 255.

Remote router group number

El número de grupo del grupo remoto al que pertenece este puerto remoto. No es necesario que los números de grupo local y remoto sean iguales.

Two-byte or one-byte station addressing

El número de bytes de la dirección de estación. La dirección de estación es la dirección SDLC del dispositivo SDLC secundario. El valor por omisión es dos bytes.

Primary or Secondary

Designa el tipo de puerto, primario (P) o secundario (S). El valor por omisión es secundario.

Configuración y supervisión de SDLC Relay

Delete

Utilice el mandato **delete** para eliminar los números de grupo, los puertos locales y los puertos remotos.

Sintaxis:

```
delete                group . . .  
                        local-port . . .  
                        remote-port
```

group *númerogrupo*
Elimina un grupo local (númerogrupo).

local-port *númerogrupo*
Elimina el puerto local para el grupo especificado.

remote-port
Elimina el puerto remoto para el grupo especificado.

Ejemplo: delete remote-port

```
Group number: [1]? 1
```

Group number

El número del grupo remoto para el puerto remoto.

Disable

Utilice el mandato **disable** para suprimir la retransmisión de todo un grupo de relay o un puerto relay específico.

Sintaxis:

```
disable                group . . .  
                        port
```

group *númerogrupo*
Suprime la transferencia de tramas SDLC Relay a un grupo específico (númerogrupo) o desde el mismo.

port Suprime la transferencia de tramas SDLC Relay a un puerto local o remoto específico o desde el mismo.

Ejemplo: disable port

```
Local group number: [1]?  
(L)ocal port or (R)emote port: [L]?
```

Group number

El número de grupo del grupo local que incluye el puerto.

Local or remote

Designa si el puerto es local o remoto.

Enable

Utilice el mandato **enable** para activar la transferencia de datos para todo un grupo o para un puerto de interfaz local específico.

Sintaxis:

```
enable  
      group . . .
```

Configuración y supervisión de SDLC Relay

<code>port</code>	
group <i>número grupo</i>	Permite la transferencia de tramas SDLC Relay al grupo local especificado (número grupo) o desde el mismo.
port	Permite la transferencia de tramas SDLC Relay al puerto local o remoto especificado o desde el mismo.
	Ejemplo: enable port
	Local group number: [1]? (L)ocal port or (R)emote port: [L]?
	Group number
	El número del grupo que incluye el puerto.
	Local or remote
	Designa si el puerto es local o remoto.

List (para red SRLY)

Utilice el mandato **list** para visualizar la configuración de la interfaz SDLC Relay (SRLY).

Sintaxis:

`list`

Ejemplo:

```
list
Maximum frame size in bytes = 2048
Encoding: NRZ
Idle State: Flag
Clocking: External
Cable Type: RS-232 DTE
Speed (bps): 0
Transmit Delay Counter: 0
```

Maximum frame size in bytes

El tamaño máximo de trama que puede enviarse a través del enlace. El tamaño máximo de trama debe ser lo suficientemente grande como para acomodar la trama mayor y la cabecera SRLY de 6 bytes.

Encoding

El esquema de codificación de transmisión para la interfaz serie. El esquema es NRZ (sin retorno a cero) o NRZI (inversión sin retorno a cero).

Idle State

El estado desocupado del enlace de datos: distintivo o marca.

Clocking

El tipo de cronometraje: interno o externo.

Cable Type

El tipo de cable de interfaz serie.

Speed (bps)

Lista la velocidad de los relojes de transmisión y recepción.

Transmit Delay Counter

Número de distintivos enviados entre tramas consecutivas.

Configuración y supervisión de SDLC Relay

List (para el protocolo SDLC Relay)

Utilice el mandato **list** para visualizar la configuración de un grupo específico o de todos los grupos.

Sintaxis:

```
list                               all
                                   group . . .
```

all Visualiza las configuraciones de todos los grupos locales.

Ejemplo: list all

SDLC/HDLC Relay Configuration

```
Local group      = 1
Group Name       = CHICAGO-TO-MIAMI
Group Type       = MULTI           Enabled      = YES
Local port       = PRIMARY         Enabled      = YES
Interface        = 2
Remote port      = SECONDARY       Enabled      = YES
Remote group     = 1               Addressing   = 2-BYTE
IP Address       = 9.67.2.3        Code level  = CURRENT

Local group      = 2
Group Name       = CHICAGO-TO-RALEIGH
Group Type       = MULTI           Enabled      = YES
Local port       = PRIMARY         Enabled      = YES
Interface        = 3
Remote port      = SECONDARY       Enabled      = YES
Remote group     = 2               Addressing   = 2-BYTE
IP Address       = 9.67.2.3        Code level  = CURRENT

Local group      = 3
Group Name       = CHICAGO-TO-PITTSBURGH
Group Type       = PT-PT           Enabled      = YES
Local port       = PRIMARY         Enabled      = YES
Interface        = 4
Remote port      = SECONDARY       Enabled      = YES
Remote group     = 3               Addressing   = 2-BYTE
IP Address       = 9.67.2.4        Code level  = CURRENT
```

Local group

Indica el número de grupo local.

Group Name

Indica el nombre de grupo local.

Group Type

Indica el tipo del grupo local, que es de punto a punto o multipunto.

Local port

Indica si el puerto es primario o secundario y su estado, habilitado o inhabilitado.

Interface

Indica el número de red o de interfaz del puerto local. Este número coincide con el número visualizado utilizando el mandato **list devices** de Config.

Remote port

Indica si el puerto remoto es primario o secundario y su estado, habilitado o inhabilitado.

Remote group

Indica el número del grupo remoto.

Addressing

Indica si se utiliza el direccionamiento de un byte o de dos bytes.

Configuración y supervisión de SDLC Relay

IP address

Indica la dirección IP interna del direccionador remoto para este grupo. Identifica el túnel IP que conecta el direccionador con el direccionador remoto.

Code level

Indica el nivel de código, actual o de migración. El nivel de código determina el rango de los números que pueden utilizarse para identificar los grupos. El nivel de código actual está en el rango de 1 a 255; el nivel de código de migración está en el rango de 0 a 15.

group *númerogrupo*

Visualiza la configuración de un grupo especificado.

Set

Utilice el mandato **set** para configurar los parámetros de la interfaz SRLY.

Sintaxis:

```
set                                cable
                                   clocking
                                   encoding
                                   frame-size
                                   idle
                                   speed
                                   transmit-delay
```

cable Establece el cable utilizado en la interfaz serie. Las opciones son:

- RS-232 DTE
- RS-232 DCE
- V35 DTE
- V35 DCE
- V36 DTE
- V36 DCE
- X21 DTE
- X21 DCE

La Tabla 86 lista los tipos de cables que puede configurar en los diversos adaptadores.

Tabla 86. Tipos de cables para las interfaces 2216

Tipo de adaptador	Tipo de cable
EIA 232 de 8 puertos	RS-232 DTE y RS-232 DCE
V.35/V36 de 6 puertos	V.35 DCE, V.35 DTE, V.36 DCE o V.36 DTE
X.21 de 8 puertos	X.21 DCE y X.21 DTE

Ejemplo:

```
set cable V35 dte
```

Se utiliza un cable DTE cuando se conecta el direccionador a algún tipo de dispositivo DCE (por ejemplo, un módem o una DSU/CSU).

Configuración y supervisión de SDLC Relay

Se utiliza un cable DCE cuando el direccionador actúa como DCE y proporciona el cronometraje para la conexión directa.

clocking *interno o externo*

Para conectar con un módem o DSU, configure el cronometraje externo y seleccione el cable DTE adecuado con el mandato **set cable**.

Para conectar directamente con otro dispositivo DTE, configure el cronometraje interno, seleccione el cable DCE adecuado con el mandato **set cable** y configure el cronometraje/velocidad de línea con el mandato **set speed**.

Valor por omisión: externo

Ejemplo:

```
set clocking internal
```

encoding *nrz o nrzi*

Configura el esquema de codificación de la interfaz SRLY como NRZ (Sin retorno a cero) o NRZI (Inversión sin retorno a cero). NRZ es el valor por omisión.

Ejemplo:

```
set encoding nrz
```

frame-size

Configura el tamaño máximo de las tramas que pueden transmitirse y recibirse en el enlace de datos. Si se establece en un valor mayor que el especificado con el mandato `add remote-secondary`, se cambia para reflejar este máximo. El IBM 2216 genera un mensaje ELS que avisa al usuario que este valor está cambiando. El usuario continuará recibiendo este mensaje ELS hasta que lo cambie en la configuración SRAM. Las entradas válidas se muestran en la Tabla 87.

Nota: El tamaño de trama debe ser lo suficientemente grande para acomodar la trama mayor recibida más una cabecera SRLY de 15 bytes.

Tabla 87. Valores válidos para el tamaño de trama en el mandato `set frame-size`

Mínimo	Máximo	Valor por omisión
128	8187	2048

idle flag

Configura el estado de desocupado de la transmisión en la interfaz SRLY. El valor por omisión es la opción de distintivo que proporciona distintivos continuados (7E hex) entre tramas.

El enlace recibirá un distintivo de desocupado transparentemente.

idle mark

Configura el estado de desocupado de la transmisión en la interfaz SRLY. La opción de marca pone la línea en estado de marca (OFF, 1) entre tramas.

El enlace recibirá una marca de desocupado transparentemente.

speed

Para el cronometraje interno, utilice este mandato para especificar la velocidad de las líneas de reloj de transmisión y recepción.

Configuración y supervisión de SDLC Relay

Para el cronometraje externo, este mandato no afecta al funcionamiento de la WAN/línea serie.

Valores válidos:

Cronometraje interno: Consulte la Tabla 88

Cronometraje externo: Consulte la Tabla 89

Tabla 88. Velocidades de línea cuando se utiliza el cronometraje interno para interfaces 2216

Tipo de adaptador	Rango de velocidades
EIA 232 de 8 puertos	De 9600 a 64 000 bps
V.35/V.36 de 6 puertos	De 9600 a 460 800 bps, 1 544 000 bps ó 2 048 000 bps
X.21 de 8 puertos	De 9600 a 460 800 bps, 1 544 000 bps ó 2 048 000 bps

Tabla 89. Velocidades de línea cuando se utiliza el cronometraje externo para interfaces 2216

Tipo de adaptador	Rango de velocidades
EIA 232 de 8 puertos	De 2400 a 64 000 bps
V.35/V.36 de 6 puertos	De 2400 a 2 048 000 bps
X.21 de 8 puertos	De 2400 a 2 048 000 bps

transmit-delay *valor*

Permite la inserción de un retardo entre paquetes transmitidos. Este mandato asegura un retardo mínimo entre tramas para que sea compatible con dispositivos serie anteriores que son más lentos del otro extremo. Este valor se especifica como el número de bytes de distintivo que deben enviarse entre tramas consecutivas. El rango es de 0 a 15. El valor por omisión es 0.

Nota: Si configura un retardo de transmisión distinto de cero para una interfaz SDLC Relay del adaptador EIA- 232E de 8 puertos, el adaptador V.35/V.36 de 6 puertos, el adaptador X.21 de 6 puertos, debe configurar la velocidad de línea utilizando el mandato **set speed**.

Acceso al entorno de supervisión SDLC Relay

Para supervisar la información relacionada con la interfaz SDLC Relay, acceda al proceso de supervisión de la interfaz realizando lo siguiente:

1. Entre el mandato **status** para buscar el PID para GWCON. (Consulte la página 9 para ver la salida de ejemplo del mandato **status**.)

2. En el indicador OPCON, entre el mandato **talk** y el PID para GWCON. Por ejemplo:

```
* talk 5  
+
```

Se visualiza el indicador GWCON (+) en la consola. Si no aparece el indicador cuando entre en GWCON, pulse **Intro** de nuevo.

3. En el indicador GWCON, entre el mandato **configuration** para ver los protocolos y las redes para los que está configurado el direccionador. Por ejemplo:

```
+ configuration
```

Configuración y supervisión de SDLC Relay

Consulte la página 120 para ver más salida de ejemplo del mandato **configuration**.

4. Entre el mandato **protocol sdlc**. Por ejemplo:

```
+ prot sdlc
SDLC Relay>
```

Se visualiza el indicador SDLC Relay en la consola. Entonces puede ver la información acerca de los grupos SDLC Relay entrando los mandatos de supervisión SDLC Relay.

Mandatos de supervisión SDLC Relay

Esta sección resume y explica los mandatos de supervisión SDLC Relay. Los mandatos de supervisión SDLC Relay le permiten ver los parámetros de las interfaces que transmiten tramas SDLC Relay. Algunos de estos mandatos como, por ejemplo, **enable** y **disable** también tienen un efecto operativo, pero no afectan a la configuración. Se visualiza el indicador SDLC Relay> para todos los mandatos de supervisión SDLC Relay. La Tabla 90 muestra los mandatos.

Tabla 90. Resumen de los mandatos de supervisión SDLC Relay

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página 10.
Clear-Port-Statistics	Borra las estadísticas de SDLC Relay para el puerto especificado.
Disable	Suprime temporalmente grupos y puertos.
Enable	Activa temporalmente grupos y puertos.
List	Visualiza las configuraciones de todo SDLC Relay y las específicas de grupos.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página 11.

Clear-Port-Statistics

Utilice el mandato **clear-port-statistics** para eliminar las estadísticas de SDLC Relay para todos los puertos. Las estadísticas incluyen contadores para los paquetes enviados y los paquetes eliminados.

Sintaxis:

clear-port-statistics

clear-port-statistics

Borra las estadísticas reunidas desde la última vez que ha reiniciado el direccionador o borrado las estadísticas.

Ejemplo:

```
clear-port-statistics
Clear all port statistics? (Yes or No): Y
```

Disable

Utilice el mandato **disable** para suprimir la transferencia de datos para todo un grupo o para un puerto relay específico. La SRAM (memoria de acceso de lectura estática) no almacena permanentemente los efectos del mandato de supervisión **disable**. Por lo tanto cuando reinicie el direccionador, se borrarán los efectos de este mandato.

Configuración y supervisión de SDLC Relay

Group Type	= PT-PT	Enabled	= YES
Local port	= PRIMARY	Enabled	= YES
Interface	= 4		
Remote port	= SECONDARY	Enabled	= YES
Remote group	= 3	Addressing	= 2-BYTE
IP Address	= 9.67.2.4	Code level	= CURRENT

Local group

Indica el número de grupo local.

Group Name

Indica el nombre de grupo local.

Group Type

Indicates the local group type, which is point-to-point or multipoint.

Local port

Indica si el puerto es primario o secundario y su estado, habilitado o inhabilitado.

Interface

Indica el número de red o de interfaz del puerto local. Este número coincide con el número visualizado utilizando el mandato **list devices** de Talk 6 o el mandato **config** de Talk 5.

Remote port

Indica si el puerto remoto es primario o secundario y su estado, habilitado o inhabilitado.

Remote group

Indica el número del grupo remoto.

Addressing

Indica si se utiliza el direccionamiento de un byte o de dos bytes.

IP address

Indica la dirección IP interna del direccionador remoto para este grupo. Identifica el túnel IP que conecta el direccionador con el direccionador remoto.

Code level

Indica el nivel de código, actual o de migración. El nivel de código determina el límite superior del rango de números que puede utilizarse para identificar los grupos.

group *númerogrupo*

Visualiza las configuraciones de un grupo especificado.

Interfaces SDLC Relay y el mandato interface de GWCON

Aunque las interfaces SDLC Relay tienen sus propios procesos de supervisión, el direccionador también visualiza estadísticas completas para las interfaces de red instaladas cuando se utiliza el mandato **interface** en el entorno GWCON. (Para obtener más información sobre el mandato **interface**, consulte la sección Capítulo 8. El proceso de operación/supervisión (GWCON - Talk 5) y sus mandatos.)

Soporte para la reconfiguración dinámica de SDLC Relay

Esta sección describe la reconfiguración dinámica (DR) en la medida en que afecta a los mandatos Talk 6 y Talk 5.

Delete Interface de CONFIG (Talk 6)

SDLC Relay soporta el mandato **delete interface** de CONFIG (Talk 6) sin ninguna restricción.

Activate Interface de GWCON (Talk 5)

SDLC Relay soporta el mandato **activate interface** de GWCON (Talk 5) sin ninguna restricción.

El mandato **activate interface** de GWCON (Talk 5) soporta todos los mandatos específicos de interfaz SDLC Relay.

Reset Interface de GWCON (Talk 5)

SDLC Relay soporta el mandato **reset interface** de GWCON (Talk 5) sin ninguna restricción.

Todos los cambios en la configuración de SDLC Relay se activan automáticamente excepto el siguiente:

Mandatos cuyos cambios no se activan por el mandato reset interface de GWCON (Talk 5)
--

CONFIG, net, set frame-size

Nota: El usuario no puede aumentar el tamaño de trama.

Configuración y supervisión de SDLC Relay

Capítulo 48. Utilización de interfaces SDLC

Este capítulo explica cómo utilizar la interfaz SDLC e incluye las secciones siguientes:

- “Procedimiento de configuración básica”
- “Configuración de interfaces de llamada de entrada SDLC conmutadas”
- “Requisitos de configuración SDLC” en la página 724

Entre los mandatos de configuración SDLC en el indicador SDLC # Config> (donde # identifica la interfaz que se especifica con el mandato network). Los cambios realizados en la configuración de los direccionadores no surten efecto inmediatamente, pero pasan a formar parte de la memoria de configuración estática del direccionador cuando se reinicia.

Procedimiento de configuración básica

Esta sección indica la configuración mínima necesaria para que DLSw o APPN puedan utilizar SDLC.

Antes de empezar cualquier procedimiento de configuración, utilice el mandato **list device** del proceso config para listar los números de las interfaz de los distintos dispositivos. En el indicador de config, seleccione la interfaz que desea configurar entrando: **network número de interfaz** o **n número de interfaz**. Si necesita más explicación sobre los mandatos de configuración, consulte los mandatos de configuración descritos en este capítulo.

Configuración de interfaces de llamada de entrada SDLC conmutadas

Una interfaz de llamada de entrada SDLC conmutada permite que un dispositivo PU de tipo 2.0 llame a un 2216 utilizando una línea SDLC conmutada, proporcionando una opción de conectividad adicional a la red. La interfaz está restringida a dispositivos PU de tipo 2.0 y sólo puede ejecutarse DLSw.

Nota: No puede configurar APPN a través de una interfaz de llamada de entrada SDLC conmutada.

Para configurar una interfaz de llamada de entrada SDLC conmutada:

1. Configure una red base V.25bis:

```
Config> set data-link v25 bis 2
Config> net 2
V25bis Config>
(configuration the V25bis net)
```

Consulte la sección “Capítulo 50. Utilización de la interfaz de red V.25bis” en la página 751 para obtener más información acerca de la configuración de V25 bis.

Nota: Cualquier parámetro de capa física como, por ejemplo, **encoding type** y **full** o bien **half duplex** se configuran en la la interfaz V.25bis y no en la interfaz de circuito de marcación SDLC conmutada.

2. Añada un dispositivo de circuito de marcación:

```
Config> add device dial
```

3. Establezca el enlace de datos para el circuito de marcación en SDLC. En este ejemplo, el circuito de marcación es la interfaz 3.

Utilización de interfaces SDLC

```
Config> set data-link sdlc 3
4. Configure el circuito de marcación:
Config> net 3
Dial circuit config> set net 2 1
Dial circuit config> encapsulator
sdlc config>
    (configure SDLC)
sdlc config> exit
Dial circuit config> exit
Config>
5. Configure DLSw:
Config> prot dls
DLSw protocol user configuration
DLSw config> add sdlc
Interface # [0]? 3
SDLC Address or 'sw' (switched dial-in) [sw]? sw 2
Source MAC address [4000112402C1]? 4000003174d2
Source SAP in hex [4]?
Destination MAC address [000000000000]? 400000000004 3
Destination SAP in hex [0]? 4 4

XID0 block num in hex (0-0xfff) [0]? 017
XID0 id num in hex (0-0xffff) [0]? 00001
For a switched dial-in link station ....
- PU type is forced to be 2
- Configured XID block/id num is used to override
  fields in the XID0 from the SDLC station
  - if block/id set to zeroes, XID0 is not modified
  - otherwise configured fields are put into XID0
- Poll type is not configured (not used)
DLSw config> li sdlc all
Net Addr  Status  Source SAP/MAC  Dest SAP/MAC  PU  Blk/IdNum  PollFrame
3  FF(sw) Enabled  04 4000003174D2  04 400000000004  2  017/00001  TEST

DLSw config> exit
Config>
```

1 No podrá establecer ningún otro parámetro de circuito de marcación y el software tomará los valores por omisión en todos los demás valores de parámetros. Para obtener información acerca de los valores por omisión, consulte la sección “Encapsulador” en la página 798.

2 La especificación de “sw” indica que se trata de una interfaz de llamada de entrada SDLC conmutada.

3 La dirección MAC de destino no puede ser sólo 0. Si especifica o toma por omisión el valor 0, el software le solicitará una dirección válida.

4 El SAP de destino no puede ser 0. Si especifica o toma por omisión el valor 0, el software le solicitará una dirección válida.

Consulte los capítulos “Utilización y configuración de DLSw” y “Supervisión de DLSw” de *Consulta de configuración y supervisión de protocolos Volumen 1* para obtener información adicional acerca de la configuración de DLSw.

Requisitos de configuración SDLC

Además de los procedimientos de configuración específicos de SDLC y los mandatos descritos en ese capítulo, es necesario configurar SDLC en el protocolo DLSw o APPN. Sólo puede ejecutarse un protocolo cada vez, DLSw o APPN, en una interfaz SDLC determinada. En otras palabras, las estaciones de enlace de una interfaz SDLC determinada no pueden dividirse entre APPN y DLSw. Si existe una configuración DLSw y una configuración APPN para la misma interfaz SDLC, el primer protocolo en activarse será el propietario de la interfaz SDLC.

Capítulo 49. Configuración y supervisión de interfaces SDLC

Este capítulo describe los mandatos de configuración y operativos SDLC. Contiene las secciones siguientes:

- “Acceso al entorno de configuración SDLC”
- “Mandatos de configuración SDLC” en la página 726
- “Acceso al entorno de supervisión SDLC” en la página 739
- “Mandatos de supervisión SDLC” en la página 739
- “Interfaces SDLC y mandato interface de GWCON” en la página 749
- “Estadísticas visualizadas para interfaces SDLC” en la página 749

Los cambios realizados en la consola de mandatos de configuración (SDLC CONFIG>) pasan a formar parte de la configuración de SRAM cuando se reinicia el direccionador.

Por el contrario, los mandatos de supervisión SDLC entrados en el proceso de supervisión SDLC surten efecto inmediatamente. Sin embargo, los cambios realizados con los mandatos de supervisión no pasan a formar parte de la configuración estática del direccionador. Cuando se reinicia el direccionador, se sobregraban los efectos de los mandatos de supervisión con la configuración estática del direccionador. La supervisión consiste en las acciones siguientes:

- La supervisión de los protocolos y las interfaces de red que actualmente utiliza el direccionador
- La realización de cambios en tiempo real en la configuración de SDLC sin que afecten de manera permanente a la configuración de SRAM
- La visualización de los mensajes ELS (Sistema de anotación cronológica de sucesos) relacionados con las actividades y el rendimiento del direccionador

Acceso al entorno de configuración SDLC

Utilice el proceso CONFIG para cambiar la configuración del direccionador. La nueva configuración surte efecto cuando se reinicia el direccionador.

Para entrar en el proceso de configuración:

1. Entre **talk 6** (o **t 6**), en el indicador OPCON (*). Esto le lleva al indicador CONFIG>, tal como muestra el ejemplo siguiente:

```
MOS Operator Console
For help using the Command Line Interface, press ESCAPE, then '?'
* talk 6
CONFIG>
```

Si no aparece el indicador CONFIG> inmediatamente, pulse la tecla **Intro** de nuevo.

Todos los mandatos de configuración SDLC se entran en el indicador SDLC config>. Puede utilizar el entorno GWCON t 5 (Consulte la sección “Capítulo 8. El proceso de operación/supervisión (GWCON - Talk 5) y sus mandatos” en la página 117) para realizar cambios dinámicos en la configuración. Sin embargo, estos cambios desaparecerán cuando se reinicie el dispositivo.

2. En el indicador Config>, entre el mandato **set data-link sdlc**. Cuando se solicite, entre el nombre de la interfaz que se ha de asociar con el dispositivo SDLC.

Configuración de interfaces SDLC

```
Config>set data-link sdlc
Interface number [0]? 2
Config>
```

- Después, entre el mandato **network**, más el número de una interfaz SDLC que ha entrado antes.

```
Config>network 2
SDLC 2 Config>
```

Consulte la sección “Capítulo 1. Introducción” en la página 3 para obtener información relacionada con el entorno de configuración.

Mandatos de configuración SDLC

Los mandatos de configuración SDLC le permiten crear o modificar la configuración de la interfaz SDLC. Esta sección resume y describe los mandatos que puede emitir desde el indicador SDLC Config> en la consola de configuración de red. Los valores por omisión para cualquier mandato y sus parámetros se visualizan en la consola, aparecen entre corchetes inmediatamente después del indicador.

Nota: Además de configurar SDLC utilizando los mandatos descritos en este capítulo, también es necesario configurar SDLC en el protocolo DLSw o APPN.

El 2216 soporta las conexiones SDLC a través de las interfaces serie RS-232, X.21 y V.35. La Tabla 91 lista los mandatos de configuración SDLC y su función.

Tabla 91. Resumen de los mandatos de configuración SDLC

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página 10.
Add	Añade una estación final SDLC. Si no se añaden específicamente las estaciones, se crearán dinámicamente con los valores por omisión cuando DLSw o APPN activen dispositivos.
Delete	Elimina una estación final SDLC.
Disable	Impide las conexiones con una de las estaciones de enlace SDLC.
Enable	Permite las conexiones con una de las estaciones de enlace SDLC.
List	Visualiza la información configurada para una de las estaciones de enlace o líneas SDLC.
Set	Configura la información específica de la estación de enlace o de la interfaz.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página 11.

Add

Utilice el mandato **add** para añadir una estación final. El direccionador es, por omisión, la estación final primaria. Si no utiliza este mandato y si ha configurado una estación SDLC en DLSw o en APPN, se añade la estación final automáticamente. El software asigna los siguientes valores por omisión a la estación:

- La BTU máxima es el máximo permitido por la interfaz
- Tx y Rx Windows son 7 para MOD 8, 127 para MOD 128

Si los valores por omisión son satisfactorios, no es necesario añadir estaciones SDLC.

Sintaxis:

add station

Ejemplo:

add station

Enter station address (in hex) [C4]?

Enter station name [SDLC_C4]?

Include station in router as secondary group poll list (Yes or [No]):

Enter router as primary group poll address (0 means disable) [00]?

Enter max packet size [2048]?

Enter "A" for 2-WAY-ALTERNATING or "S" for 2-WAY-SIMULTANEOUS [S]?

Enter router as secondary link station poll pause [0]?

Enter receive window [7]?

Enter transmit window [7]?

Enter station address

La dirección SDLC de la estación en el rango de 01 a FE.

Enter station name

La designación de nombre de la estación SDLC (los caracteres máximos son 8).

Include station in router as secondary group poll list

Seleccione si se ha de incluir o no esta estación en la lista de sondeo de grupo secundario para esta interfaz. El software SDLC soporta la función de sondeo de grupo IBM 3174 para la estación secundaria SDLC. Debe añadir una dirección de sondeo de grupo utilizando el mandato **set link group-poll** para que este parámetro surta efecto.

Enter router as primary group poll address (0 means disable)

Especifica la dirección de grupo que se ha de sondear. La Dirección de sondeo de grupo primario se entra por cada estación.

Valores válidos: De X'00' a X'FE', donde 0 indica la no utilización del sondeo de grupo

Valor por omisión: X'00'

Enter max packet size

El tamaño máximo de paquete que se puede enviar o recibir en la estación de enlace remota. Este valor no puede ser mayor que el especificado para el enlace. Este valor se configura con el mandato **set link frame-size**.

Enter "A" for 2-WAY-ALTERNATING or "S" for 2-WAY-SIMULTANEOUS

Especifica si la estación de enlace funciona en modalidad bidireccional simultánea o bidireccional alternativa. El valor por omisión se hereda de la configuración de la interfaz.

Enter router as secondary link station poll pause

Especifica el período de tiempo que una estación secundaria retardará el envío del final del sondeo después de haberse sondeado.

Notas:

1. Este valor debe ser menor que el tiempo de espera excedido de sondeo para la estación primaria.
2. Los valores distintos de 0 en enlaces multipunto pueden provocar un tiempo pobre de respuesta.

Valores válidos: De 0 a 25,5 segundos en incrementos de 0,1 segundo

Valor por omisión: 0

List

Utilice el mandato **list** para visualizar la información de configuración sobre una o todas las estaciones de enlace SDLC.

Sintaxis:

```
list          link
              station nombre o all
```

link Visualiza la configuración de la interfaz SDLC.

Ejemplo:

```
list link
Link configuration for: LNK00001 (ENABLED)

Role:          PRIMARY          Type:          POINT-TO-POINT
Modulo:        8                Frame Size:    2048
Sc Gp Poll:    00              Dflt protcl:  ALTERNATE

Timers:        XID/TEST response: 2.0 sec
                SNRM response:    2.0 sec
                Poll response:     2.0 sec
                Inter-poll delay:  0.0
                Primary poll pause: 0.5 sec
                Dflt sec poll pause: DISABLED
                RTS hold delay:     DISABLED
                Inactivity timeout: 30.0 sec

Counters:      XID/TEST retry:    8
                SNRM retry:        6
                Poll retry:         10
SDLC 1 Config>
```

Link configuration

El nombre y el estado de la estación de enlace SDLC que están en la configuración del direccionador.

Role La función primaria, secundaria o negociable para las estaciones de enlace que configura utilizando el mandato **set link role**.

Type El tipo de enlace, multipunto o de punto a punto. Si **role** es *secundaria*, el valor *multipunto* para este parámetro hace que RTS se desactive cuando no se transmite.

Duplex

Especifica la posibilidad de línea del hardware. Para la gestión de un enlace simultáneo bidireccional, es necesaria la posibilidad de hardware *dúplex*.

Modulo

El rango de número de secuencia que se ha de utilizar en el enlace: MOD 8 (0-7) o MOD 128 (0 - 127).

Idle state

El patrón de bits (FLAG o MARK) transmitido en la línea cuando la interfaz no transmite datos.

Speed La velocidad de datos físicos de la red. Cuando el cronometraje es interno, es la velocidad de datos generada por el reloj interno. Este parámetro no tiene efecto para líneas cronometradas externamente.

Group Poll

Dirección utilizada para la característica de sondeo de grupo. Las estaciones que tienen codificada la inclusión de grupo como *sí* responderán a los sondeos no numerados recibidos de esta dirección. Esta dirección no debe ser cero para que la característica de sondeo de grupo surta efecto

Configuración de interfaces SDLC

para cualquier estación secundaria bajo este enlace. Cada estación secundaria tendrá una dirección de estación específica además de la dirección de grupo.

Cable Especifica el tipo de cable que se utiliza (RS-232, V.35, V.36 ó X.21).

Encoding

Configura el esquema de codificación de la transmisión SDLC como NRZ (Sin retorno a cero) o NRZI (Inversión sin retorno a cero).

Clocking

Cronometraje de interfaz, externo o interno.

Frame Size

El tamaño máximo de trama que puede enviarse a través de la interfaz.

Timers:

Todos los temporizadores listados más abajo tienen una resolución de 100 ms.

XID/TEST resp.

El tiempo que se ha de esperar un mensaje de respuesta XID o TEST antes de retransmitir la trama XID o TEST. El valor 0 indica que el direccionador no retardará el reintento después de su siguiente turno de la lista de sondeo.

SNRM response

El tiempo máximo que se ha de esperar un mensaje de respuesta UA antes de que la estación retrasmitea SNRM(E).

Poll response

El tiempo máximo que se ha de esperar una respuesta de una estación sondeada antes de reintentarlo.

Inter-poll delay

El período de tiempo que el direccionador (con una función primaria) espera después de recibir una respuesta, antes de sondear la siguiente estación.

Nota: El temporizador de Pausa de sondeo primario es el temporizador de sondeo preferido. El Retardo entre sondeos provoca problemas de tiempos de respuesta del usuario final. Consulte la página 735 para obtener más información acerca de la pausa de sondeo primario.

Interframe delay

Especifica un período de tiempo para inyectar distintivos entre tramas. El valor máximo de 120 inyecta aproximadamente 15 distintivos entre tramas para una línea de 9600 baudios.

Leading Flags

El número de distintivos enviados si el retardo entre tramas no es suficiente responder al dispositivo del otro extremo del enlace. Se trata de una unidad de tiempo con un valor máximo de 100.

Inactivity timeout

Para estaciones secundarias NRM/E desocupadas, establece el tiempo después del cual la interfaz cambia la estación a su estado de recuperación. Un 0 (cero) hace que la estación permanezca desocupada permanentemente.

Counters:

XID/TEST retry

El número máximo de veces que el direccionador envía una trama XID o TEST sin recibir una respuesta antes de exceder el tiempo de espera. El valor 0 indica que el direccionador lo reintentará indefinidamente.

SNRM El número máximo de veces que el direccionador enviará una trama SNRM(E) sin recibir una respuesta antes de exceder el tiempo de espera. El valor 0 indica que el direccionador lo reintentará indefinidamente.

Poll retry

El número máximo de veces que el direccionador sondea la estación sin recibir una respuesta antes de exceder el tiempo de espera. El valor 0 indica que el direccionador continuará reintentándolo indefinidamente.

Nota: Los parámetros de capa física como, por ejemplo, **duplex type**, **speed**, **cable type**, **encoding**, **clocking**, **leading flags** y **inter-frame delay** no se aplican para interfaces de circuitos de marcación SDLC y no se visualizan con el mandato **list link**.

station todas o dirección o nombre de estación de enlace

Visualiza información para la estación de enlace SDLC especificada o para todas las estaciones de enlace.

Ejemplo:

```
list station c1
Addr-A/S      Status  Max BTU  Rx Window  Tx Window  Secondary Poll Pause  Primary GP Addr
(Sec Gp)  Name
-----
C1   A SDLC_C1  ENABLED   2048       7         7         0.0 sec   00
```

Ejemplo:

```
list station all
Addr-A/S      Status  Max BTU  Rx Window  Tx Window  Secondary Poll Pause  Primary GP Addr
(Sec Gp)  Name
-----
C1   A SDLC_C1  ENABLED   2048       7         7         0.0 sec   00
C2   A SDLC_C2  ENABLED   2048       1         7         0.0 sec   00
```

Address

La dirección de la estación de enlace SDLC. La dirección entre paréntesis es la Dirección del grupo del "direccionador como secundario" de la interfaz que utiliza la estación si ésta tiene establecida la inclusión de grupo, el enlace es secundario y la dirección del grupo secundario no es cero.

Name La designación de nombre de serie de caracteres de la estación de enlace SDLC.

Status

El estado de la estación de enlace SDLC, ENABLED o DISABLED.

Max BTU

El límite de tamaño de trama de la estación. Este tamaño de trama no debe ser mayor que el tamaño de paquete de la Unidad básica de transmisión (BTU) configurado con el mandato **set link frame-size**.

Rx Window

El tamaño de la ventana de recepción.

Tx Window

El tamaño de la ventana de transmisión.

Configuración de interfaces SDLC

Set

Utilice el mandato **set** para configurar información específica para una o todas las estaciones de enlace SDLC.

Sintaxis:

```
set                               link
                                     cable*
                                     clocking*
                                     duplex* . . .
                                     encoding* . . .
                                     frame-size
                                     group poll* ...
                                     idle* . . .
                                     inactivity ...
                                     inter-frame delay*
                                     leading flags*
                                     modulo . . .
                                     name
                                     poll . . .
                                     role* . . .
                                     snrm
                                     speed*
                                     type* . . .
                                     xid/test
                                     station
                                     address. . .
                                     group-inclusion
                                     gp-address-prim
                                     max-packet
                                     name
                                     protocol
                                     receive-window
                                     secondary-phase
                                     transmit-window
```

***Nota:** Estos mandatos no están disponibles para las interfaces del circuito de marcación SDLC.

link cable *tipo*

Establece el cable conectado a esta interfaz. Las opciones son los tipos de DCE y DTE siguientes: V.36, RS-232, V.35 y X.21.

Configuración de interfaces SDLC

La Tabla 92 lista los tipos de cables que puede configurar en los diversos adaptadores.

Tabla 92. Tipos de cables para interfaces 2216

Tipo de adaptador	Tipo de cable
EIA 232 de 8 puertos	RS-232 DTE y RS-232 DCE
V.35/V36 de 6 puertos	V.35 DCE, V.35 DTE, V.36 DCE o V.36 DTE
X.21 de 8 puertos	X.21 DCE y X.21 DTE

Se utiliza un cable DTE cuando se conecta el direccionador a algún tipo de dispositivo DCE (por ejemplo, un módem o una DSU/CSU).

Se utiliza un cable DCE cuando el direccionador actúa como DCE y proporciona el cronometraje para la conexión directa.

link clocking *interno o externo*

Para conectar un módem o DSU, configure el cronometraje externo y seleccione el cable DTE adecuado con el mandato **set link cable**.

Para conectar directamente con otro dispositivo DTE, configure el cronometraje interno, seleccione el cable DCE adecuado con el mandato **set link cable** y configure el cronometraje/velocidad de línea con el mandato **set link speed**.

Valor por omisión: externo

link duplex *dúplex o semi-dúplex*

Configura la línea SDLC para la señalización *dúplex* o *semi-dúplex*. *Dúplex* significa que el 2216 activa la RTS y espera ver la señal CTS antes de transmitir datos. *Semi-dúplex* significa que el 2216 no espera que se active la señal CTS antes de transmitir datos.

Nota: El tipo de dúplex no controla cómo funciona SDLC a nivel de protocolo SDLC (bidireccional simultáneo o bidireccional alternativo).

link encoding *nrz o nrzi*

Configura el esquema de codificación de la transmisión SDLC como NRZ (Sin retorno a cero) o NRZI (Inversión sin retorno a cero). NRZ es el valor por omisión.

link frame-size

Configura el tamaño máximo de las tramas que pueden transmitirse y recibirse en el enlace de datos. Las entradas válidas se muestran en la Tabla 93.

Tabla 93. Valores válidos para el tamaño de trama en el mandato link frame-size

Mínimo	Máximo	Valor por omisión
128	8187	2048

Establezca el tamaño de trama del enlace en un tamaño igual o superior al tamaño máximo de paquete que ha configurado con el mandato **set station xxx max packet**. De lo contrario, el direccionador restablece automáticamente el tamaño máximo de paquete al tamaño de trama del enlace y emite el mensaje siguiente ELS:

```
SDLC.054: nt 3 SDLC/0 Stn xx-MaxBTU too large for Link adjusted (4096->2048)
```

Ejemplo: set link frame-size

Configuración de interfaces SDLC

Frame size in bytes (128 - 8187) [2048]?

link group-poll

Establece una dirección de sondeo de grupo para el direccionador como estaciones secundarias del enlace. El software SDLC soporta la función de sondeo de grupo IBM 3174. Utilice el mandato **add station** o el mandato **set station group inclusion** para incluir una estación en la lista de sondeo de grupo.

Ejemplo:

```
set link group-poll
Enter group poll address router as secondary (in hex) [00:]?f3
Group poll support enabled
```

link idle flag

Configura el estado de desocupado de la transmisión para la trama SDLC. El valor por omisión es la opción de distintivo que proporciona distintivos continuados (7E) entre tramas.

Ejemplo: set link idle flag

El enlace recibirá un distintivo de desocupado transparentemente.

link idle mark

Configura el estado de desocupado de la transmisión para la trama SDLC. La opción de marca pone la línea en estado de marca (OFF, 1) entre tramas.

link inactivity *número-de-segundos*

Para estaciones secundarias NRM/E desocupadas, establece el tiempo después del cual la interfaz cambia la estación a su estado de recuperación. El rango es de 0 a 7200 segundos. El valor por omisión es 30. Un 0 (cero) hace que la estación permanezca desocupada permanentemente.

Ejemplo:

```
set link inactivity
Enter secondary link station inactivity timeout :[30.0]?
```

link inter-frame delay

Permite la inserción de un retardo entre los paquetes transmitidos. Este mandato asegura un mínimo de retardo entre tramas para la compatibilidad con los dispositivos serie más antiguos y lentos del otro extremo. Este parámetro es el período de tiempo entre tramas.

Valores válidos: De 0 a 120

Valor por omisión: 0

Ejemplo:

```
set link inter-frame
Transmit Delay Counter [0]?
```

link leading flags

Establece el número de distintivos iniciales. Utilice este mandato cuando el retardo entre tramas no sea suficiente para permitir una respuesta del 2216 a otro dispositivo. Este mandato también debe utilizarse para establecer un retardo de distintivos iniciales si está utilizando módems semi-dúplex que no tienen la posibilidad de recibir un paquete en cuanto el módem activa la señal de módem CTS.

Valores válidos: 0 a 100

Valor por omisión: 0

Ejemplo:

```
set link leading flags
Leading flags delay [0]?
```

link modulo 8 or 128

Especifica el rango de números de secuencia que se ha de utilizar en el enlace: MOD 8 (de 0 a 7) o MOD 128 (de 0 a 127). El valor por omisión es MOD 8.

Nota: Cuando cambie este valor, el tamaño de ventana se convierte en no válido. Utilice el mandato **set station** para cambiar los tamaños de la ventana de recepción y la ventana de transmisión. Los tamaños de ventana válidos son de 0 a 7.

También, cuando **link modulo** es 128, se utiliza SNRME en lugar de SNRM en el arranque de conexión y las cabeceras de tramas de supervisión se expanden con un byte adicional.

link name

Establece una serie de caracteres para el enlace que está configurando. Este parámetro sólo tiene finalidad informativa.

Ejemplo:

```
set link name
Enter link name: [LINK_0]?
```

link poll delay

Establece el retardo de tiempo entre cada sondeo que se envía a través de la interfaz. **link poll delay** es menos preferido que **link poll ppause**. **link poll delay** establece un retardo entre cada sondeo y, por lo tanto, causa problemas de tiempo de respuesta incluso cuando el enlace se utiliza poco. Si **link poll ppause** se establece en > 0, **link poll delay** debe establecerse en 0.

Ejemplo:

```
set link poll delay
Enter delay between polls [0]?
```

También puede utilizar el mandato de t 5, set link poll ppause, para establecer **primary poll pause**.

link poll ppause

Establece la pausa de sondeo primario.

Este parámetro determina el tiempo mínimo para reiniciar el ciclo de sondeo. Por ejemplo, si hay 5 estaciones en un enlace multidesactivado y las 5 estaciones se sondean en 0,2 segundos y PPAUSE se establece en 0,5 segundos, el sondeo de la primera estación esperará 0,3 segundos más. Si se han recibido datos de diversas estaciones, el tiempo en completar el sondeo de las 5 estaciones probablemente será mayor que 0,5 segundos y el sondeo de la primera estación no se retrasaría.

Ejemplo:

```
set link poll ppause
Enter delay between polls [0.5]?
```

link poll retry

Establece el número de veces que la interfaz reintenta sondear la estación de enlace SDLC secundaria antes que cierre la conexión.

Ejemplo:

Configuración de interfaces SDLC

```
set link poll retry
Enter poll retry count (0 = forever) [10]?
```

link poll timeout

Establece el período de tiempo que la interfaz espera una respuesta de sondeo antes de exceder el tiempo de espera.

Ejemplo:

```
set link poll timeout
Enter poll timeout [2.0]?
```

link role *primaria* o *secundaria* o *negociable*

Configura la interfaz como una estación de enlace primaria, secundaria o negociable (el valor por omisión es primaria).

Notas:

1. Para DLSw, **negotiable** utiliza X'FF' (dirección de difusión) para el sondeo inicial.
Cuando se utiliza la dirección de difusión para negociar la función, el enlace utiliza inicialmente una configuración SDLC por omisión y, después, la resuelve en una estación configurada, si la dirección específica coincide.
Cuando **primary** es la función del enlace, éste realiza un sondeo inicial para una dirección específica.
2. Para APPN de punto a punto o negociable, se utiliza la dirección de difusión para el sondeo inicial. Para el multipunto primario, se utiliza la dirección específica.
3. Para SDLC conmutado, el dispositivo debe ser primario, de modo que **link role type** no es configurable para las interfaces de circuito de marcación SDLC.

link snrm *tiempo de espera excedido* o *reintento*

Configura la información SNRM(E) siguiente para las estaciones primarias:

timeout

El tiempo que se ha de esperar una respuesta de Reconocimientos sin numerar (UA) antes de retransmitir un SNRM(E).

retry El número de veces que se ha de retransmitir un SNRM(E) sin recibir una respuesta antes de abandonar.

Ejemplo:

```
set link snrm timeout
Enter SNRM response timeout [2.0]?
```

Ejemplo:

```
set link snrm retry
Enter SNRM retry count (0=forever) [6]?
```

link speed

Para el cronometraje interno, utilice este mandato para especificar la velocidad de las líneas de reloj de transmisión y recepción.

Para el cronometraje externo, este mandato no afecta al funcionamiento de la WAN/línea serie.

Valores válidos:

Cronometraje interno: Consulte la Tabla 94 en la página 737

Cronometraje externo: Consulte la Tabla 95 en la página 737

Configuración de interfaces SDLC

Tabla 94. Velocidades de línea cuando se utiliza el cronometraje interno para interfaces 2216

Tipo de adaptador	Rango de velocidades
EIA 232 de 8 puertos	De 9600 a 64 000 bps
V.35/V.36 de 6 puertos	De 9600 a 460 800 bps, 1 544 000 bps ó 2 048 000 bps
X.21 de 8 puertos	De 9600 a 460 800 bps, 1 544 000 bps ó 2 048 000 bps

Tabla 95. Velocidades de línea cuando se utiliza el cronometraje externo para interfaces 2216

Tipo de adaptador	Rango de velocidades
EIA 232 de 8 puertos	De 2400 a 64 000 bps
V.35/V.36 de 6 puertos	De 2400 a 2 048 000 bps
X.21 de 8 puertos	De 2400 a 2 048 000 bps

Ejemplo:

```
set link speed  
Line Speed [64000]?
```

link type *multipunto* o *de punto a punto*

Configura el enlace SDLC para un enlace multipunto o un enlace de punto a punto. Si el direccionador es secundario, este parámetro determina si se controla RTS.

Nota: Para SDLC conmutado, el enlace es siempre de punto a punto, de modo que **link type** no es configurable para las interfaces de circuito de marcación SDLC.

link xid/test *tiempo de espera excedido* o *reintento*

Configura la información de XID/prueba siguiente para las estaciones primarias:

timeout

La cantidad máxima de tiempo que se ha de esperar para una respuesta de trama XID o TEST antes de retransmitir la trama XID o TEST.

retry El número máximo de veces que una trama XID o TEST se vuelve a enviar antes de dejarlo. Un 0 (cero) hace que el direccionador lo reintente indefinidamente.

remote-secondary *dirección* o *dirección nombre_estación_enlace* <argumento>

Cambia la dirección de la estación remota en el rango de 02 a FE.

Ejemplo: set remote-secondary SDLC_C1 address ce

station *dirección* o *nombre* address

Cambia la dirección SDLC de la estación en el rango de 01 a FE.

Ejemplo:

```
set station c1 address  
Enter station address (in hex) [C1]?
```

station *dirección* o *nombre estación de enlace* group-inclusion *no* o *sí*

Para estaciones secundarias SDLC, establezca si se ha de incluir esta estación en la lista de sondeo de grupo para este enlace. Para que esto sea efectivo, añada una dirección de sondeo de grupo secundario utilizando el mandato **set link group-poll**.

Configuración de interfaces SDLC

Ejemplo: `set station c1 group-inclusion yes`

station gr-address-prim

Especifica el direccionador como la dirección de grupo primario que se ha de sondear. Una dirección específica no puede utilizarse también como dirección de grupo.

Valores válidos: De X'00' a X'FE', donde X'00' indica que no se utiliza el sondeo de grupo

Valor por omisión: X'00'

station dirección o nombre max-packet

El tamaño máximo del paquete que la estación puede recibir (valor por omisión: 2048). No establezca un tamaño máximo de paquete mayor que el tamaño de trama de enlace que se configura con el mandato **set link frame-size**; si lo hace, el direccionador restablece automáticamente el tamaño máximo de paquete en el tamaño de trama de enlace y emite el mensaje ELS siguiente:

```
SDLC.054: nt 3 SDLC/0 Stn xx-MaxBTU too large for Link adjusted (4096->2048)
```

Ejemplo:

```
set station c1 max-packet
Enter max packet size [2048]?
```

station dirección o nombre name

El nombre de la estación SDLC.

Ejemplo:

```
set station c1 name
Enter station name [SDLC_C1]?
```

station protocol

Define si la estación se ejecuta como bidireccional alternativa (TWA) o bidireccional simultánea (TWS).

Nota: TWS necesita hardware dúplex.

station dirección o nombre receive window

El número máximo de tramas que el direccionador puede recibir antes de enviar una respuesta. El rango es de 1 a 7. El valor por omisión es 7.

Ejemplo:

```
set station c1 receive-window
Enter receive window [7]?
```

Nota: Asegúrese de que el tamaño de ventana de recepción es lo suficientemente grande, porque el direccionador desconectará la estación si se excede el tamaño de ventana. Establezca la **receive window** en el valor máximo para el módulo configurado.

station secondary-pause

Especifica el período de tiempo que la estación secundaria retrasará el envío del final del sondeo después de que se haya sondeado.

Notas:

1. Este valor debe ser menor que el tiempo de espera excedido de sondeo para la estación primaria.
2. Los valores mayores que 0 en enlaces multipunto pueden provocar tiempos de respuesta pobres.

Configuración de interfaces SDLC

Valores válidos: De 0 a 25,5 segundos en incrementos de 0,1 segundo. Un valor mayor que 0 es más útil en enlaces de punto a punto TWS ya que permite que ambas direcciones envíen a la vez.

Valor por omisión: 0

station *dirección o nombre* **transmit-window**

El número máximo de tramas que el direccionador puede transmitir antes de recibir una trama de respuesta. El rango para MOD 8 es de 1 a 7. El rango para MOD 128 es de 8 a 127.

Ejemplo:

```
set station c1 transmit-window
Enter transmit window [7]?
```

Acceso al entorno de supervisión SDLC

El entorno de supervisión es el proceso GWCON. Para entrar en el proceso GWCON:

1. Entre **talk 5** (o **t 5**) en el indicador OPCON (*). Esto le lleva al indicador GWCON (+), tal como se muestra en el ejemplo:

```
MOS Operator Console
```

```
For help using the Command Line Interface, press ESCAPE, then '?'
```

```
* talk 5
+
```

2. Después, entre el mandato **network número** utilizando el número que identifica la interfaz que previamente ha configurado para el dispositivo SDLC.

```
+ network 2
SDLC Console
SDLC-2>
```

Todos los mandatos GWCON (Supervisión) se entran en el indicador +.

Consulte la sección “Capítulo 1. Introducción” en la página 3 para obtener información relacionada con el entorno de supervisión.

Mandatos de supervisión SDLC

Esta sección resume y explica la consola SDLC y los mandatos relacionados. Utilice estos mandatos para reunir información de la base de datos. La Tabla 96 lista los mandatos de supervisión SDLC y su función.

Tabla 96. Resumen de los mandatos de supervisión SDLC

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página 10.
Add	Añade una estación de enlace SDLC
Clear	Borra los contadores de la interfaz SDLC.
Delete	Elimina dinámicamente una estación de enlace SDLC.
Disable	Inhabilita las conexiones con una estación de enlace SDLC.
Enable	Habilita las conexiones con una estación de enlace SDLC.
List	Visualiza las configuraciones de las estaciones de enlace SDLC y la información de estación de enlace.

Supervisión de interfaces SDLC

Tabla 96. Resumen de los mandatos de supervisión SDLC (continuación)

Mandato	Función
Msgsz	Permite la supervisión de bytes en los datos no visibles de otra manera. Se pueden visualizar entre entre 12 y 50 bytes para los mensajes ELS de SDLC 50 a 53.
Set	Configura la información de la estación de enlace y la interfaz específica.
Test	Prueba el enlace entre el direccionador y la estación de enlace SDLC.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página 11.

Add

Utilice el mandato **add** para añadir una estación final. El direccionador es, por omisión, la estación final primaria. Si no utiliza este mandato y si ha configurado una estación SDLC en DLSw o APPN, la estación final se añade automáticamente.

Sintaxis:

add station

Para ver un ejemplo e información adicional sobre el mandato **add**, consulte la sección "Add" en la página 726.

Clear

Utilice el mandato **clear** para borrar los contadores para la interfaz, para una estación o para todas las estaciones. Utilice el mandato **list all stations** para listar las estaciones.

Sintaxis: **clear** link
station ...

link *nombre o dirección*

Borra los contadores para una interfaz SDLC.

station *nombre o dirección o all*

Borra los contadores para una estación específica o para todas las estaciones.

Delete

Utilice el mandato **delete** para terminar una conexión SDLC existente sin afectar a la configuración SDLC de SRAM. Este mandato termina cualquier sesión SDLC que pueda haber en proceso en la estación de enlace. El direccionador se considera la estación final primaria por omisión.

Sintaxis:

delete station nombre o dirección

Disable

Utilice el mandato **disable** para inhabilitar el establecimiento de conexión en una o todas las estaciones de enlace SDLC sin afectar a la configuración SDLC de SRAM. El mandato **disable** también termina cualquier conexión existente con la estación.

Sintaxis: **disable** link

station . . .

link Impide la conexión en todas las estaciones de enlace SDLC configuradas en la interfaz terminando todas las conexiones.

station *nombre o dirección*

Impide la conexión en la estación final especificada (nombre de estación de enlace) terminando cualquier conexión existente.

Enable

Utilice el mandato **enable** para habilitar el establecimiento de conexión con las estaciones de enlace SDLC remotas sin afectar a la SRAM de configuración de SDLC.

Sintaxis:

enable link
station . . .

link Permite que los subsistemas (por ejemplo, DLSw) utilicen los recursos de SDLC.

station *nombre o dirección*

Permite conexiones con la estación final especificada.

List

Utilice el mandato **list** para visualizar las estadísticas específicas de la capa de enlace de datos y de la interfaz.

Sintaxis:

list link configuration
link counters
station . . .

link configuration

Visualiza la información para todas las estaciones de enlace SDLC configuradas en la interfaz.

Para ver un ejemplo e información adicional sobre el mandato **list**, consulte la sección "List" en la página 729.

link counters

Visualiza información para los contadores SDLC desde el último reinicio del direccionador o desde la última vez que se han borrado los contadores.

I-Frames

Número total de tramas de información recibidas y transmitidas.

I-Bytes

Número total de bytes de información recibidos y transmitidos.

Re-Xmit

Número total de tramas que se han retransmitido.

UI-Frames

Número total de tramas de información no numerada recibidas y transmitidas.

Supervisión de interfaces SDLC

UI-Bytes

Número total de bytes de información no numerada recibidos y transmitidos.

RR Número total de Recepciones preparadas (RR) recibidas y transmitidas.

RNR Número total de Recepciones no preparadas (RNR) recibidas y transmitidas.

REJ Número total de Rechazos recibidos y transmitidos.

UP Sondeos no numerados (sondeo de grupo) recibidos y transmitidos.

station todas o dirección o nombre de estación de enlace

Visualiza el estado de la estación de enlace SDLC especificada o de todas las estaciones. El software visualiza un * junto a las estaciones que no se han configurado explícitamente utilizando el mandato **add station** pero que se han añadido a la configuración porque se han definido y activado en la capa de protocolo (DLSw o APPN).

Visualiza información para la estación de enlace SDLC especificada (nombre de estación de enlace) de la interfaz.

Address

La dirección de la estación de enlace SDLC. La dirección entre paréntesis es la dirección del grupo de la estación. (00) indica que no se ha definido una dirección de grupo.

Name La designación de nombre de serie de caracteres de la estación de enlace SDLC.

Status

El estado de la estación de enlace SDLC:

Enabled

Habilitada, pero no asignada

Idle Asignada, pero no se utiliza

Connected

Conectada

Disconnected

Desconectada

Connecting

Establecimiento de conexión en proceso.

Discnectng

Desconexión en proceso

Recovering

Intentando la recuperación de un error de enlace de datos temporal.

Max BTU

El límite de tamaño de trama de la estación remota. Este tamaño de trama no debe ser mayor que el tamaño de paquete de la Unidad básica de transmisión (BTU) configurado con el mandato **set link frame-size**. El valor por omisión es 2048 bytes.

Supervisión de interfaces SDLC

Rx Window

El tamaño de la ventana de recepción.

Tx Window

El tamaño de la ventana de transmisión.

station nombre o dirección counters

Visualiza las cuentas de transmisión y recepción de tramas para la estación de enlace especificada.

I-Frames

Número de tramas de información recibidas y transmitidas

I-Bytes

Número de bytes de información recibidos y transmitidos

Re-Xmit

Número de tramas retransmitidas

UI-Frames

Número de tramas de Información no numerada recibidas y transmitidas

UI-Bytes

Número de bytes de Información no numerada recibidos y transmitidos

XID-Frames

Número de tramas de Identificación de intercambio recibidas y transmitidas

RR Número de tramas de Recepción preparada recibidas y transmitidas

RNR Número de tramas de Recepción no preparada recibidas y transmitidas

REJ Número de Rechazos recibidos y transmitidos

TEST Número de tramas de Prueba recibidas y transmitidas

SNRM Número de tramas de Establecer modalidad de respuesta normal recibidas y transmitidas

DISC Número de tramas de Desconexión recibidas y transmitidas

UA Número de tramas de Reconocimiento no numerado recibidas y transmitidas

DM Número de tramas de Modalidad desconectada recibidas y transmitidas

FRMR Número de tramas de Rechazo de tramas recibidas y transmitidas

UP Sondeos no numerados (sondeo de grupo) recibidos y transmitidos.

Ejemplo:

```
SDLC-2> list link counters
      I-Frames  I-Bytes  Re-Xmit  UI-Frames  UI-Bytes
      -----  -
Send      0          0          0          0          0
Recv      0          0
      RR      RNR      REJ      UP
```

Supervisión de interfaces SDLC

```

-----
Send      0      0      0      0
Recv      0      0      0      0

SDLC-2> list station c1
Addr-A/S  Name      Status  Max BTU  Rx  Tx  Secondary  Primary
(Sec Gp)  Name      Status  Max BTU  Win Win  Poll Pause  GP Addr
-----
C1   A SDLC_C1  ENABLED  2048    7   7   0.0 sec  00

```

Ejemplo:

```

SDLC-2> list station all

Addr-A/S  Name      Status  Max BTU  Rx  Tx  Secondary  Primary
(Sec Gp)  Name      Status  Max BTU  Win Win  Poll Pause  GP Addr
-----
C1   A SDLC_C1  ENABLED  2048    7   7   0.0 sec  00
C2   A SDLC_C2  ENABLED  2048    1   7   0.0 sec  00

```

Ejemplo:

```

SDLC-2> list station c1 counters
      I-Frames  I-Bytes  Re-Xmit  UI-Frames  UI-Bytes  XID-Frames
-----
Send      9      384      0      0      0      6
Recv     29     42792    0      0      0      3

      RR      RNR      REJ      TEST      SNRM      DISC
-----
Send     598      0      0      0      1      0
Recv     587      0      0      0      0      0

      UA      DM      FRMR      UP
-----
Send      0      0      0      0
Recv      1      0      0      0

```

Msgsz

Utilice el mandato **msgsz** para visualizar entre 12 y 50 bytes de los mensajes ELS de SDLC 50 a 53.

Sintaxis:

msgsz

Enter between 12 and 50 bytes

Especifica el número de bytes que se han de visualizar. El valor por omisión es 12 bytes.

Set

Utilice el mandato **set** para configurar dinámicamente la información específica de una o todas las estaciones de enlace SDLC sin afectar a la configuración de SRAM. En el entorno de supervisión SDLC, el mandato **set** sólo puede ejecutarse en enlaces o estaciones inhabilitados. Todos los valores de tiempo se entran en segundos, con una resolución de 0,1 segundo.

Sintaxis:

```

set                               link

                                     group poll* ...
                                     inactivity ...
                                     modulo . . .
                                     name
                                     poll . . .

```

Supervisión de interfaces SDLC

protocol . . .
role* . . .
secondary-pause . . .
snrm
type* . . .
xid/test
station
address. . .
group-inclusion
gp-address-prim
max-packet
name
protocol
receive-window
secondary-pause
transmit-window

***Nota:** Estos mandatos no están soportados en interfaces de circuitos de marcación SDLC.

link group-poll *dirección*

Establece una dirección de sondeo de grupo para las estaciones secundarias del enlace. El software SDLC soporta la función de sondeo de grupo IBM 3174. Utilice el mandato **add station** o el mandato **set station group inclusion** para incluir una estación en la lista de sondeo de grupo.

Ejemplo:

```
set link group-poll
Enter group poll address (in hex) [00:]?f3
Group poll support enabled
```

link inactivity

Para estaciones secundarias NRM/E desocupadas, establece el tiempo después del cual la interfaz cambia la estación a su estado de recuperación. El rango es de 0 a 7200 segundos. El valor por omisión es 30. Un 0 (cero) hace que la estación permanezca desocupada permanentemente.

Ejemplo:

```
set link inactivity
Enter secondary link station inactivity timeout :[30.0]?
```

link modulo

Cambia dinámicamente el rango de los números de secuencia que se han de utilizar en el enlace de datos sin afectar a la configuración de SRAM. El módulo 8 especifica un rango de números de secuencia del 0 al 7 y el módulo 128 especifica del 0 al 127. El valor por omisión es 8.

Nota: Cuando cambie este valor, los tamaños de ventana de transmisión y recepción se convierten en no válidos. Utilice el mandato **set station** para cambiar los tamaños de ventana de recepción y de ventana de transmisión.

Supervisión de interfaces SDLC

link name

Cambia dinámicamente el nombre del enlace sin afectar a la configuración de SRAM. Pueden entrarse un máximo de 8 caracteres. Este parámetro sólo tiene finalidad informativa.

Ejemplo:

```
set link name
Enter link name: [LINK_0]?
```

link poll delay or timeout or retry

Cambia dinámicamente la siguiente información de sondeo sin afectar a la configuración de SRAM.

delay Configura el retardo entre cada sondeo que se envía a través de la interfaz.

timeout

Configura el período de tiempo que el direccionador espera una respuesta de sondeo antes de exceder el tiempo de espera.

retry Configura el número de veces que la interfaz reintenta sondear la estación de enlace SDLC remota antes de cerrar la conexión.

Ejemplo:

```
set link poll delay
Enter delay between polls [0.2]?
```

link protocol

Define si la estación se ejecuta como TWA o TWS.

Nota: TWS necesita hardware dúplex.

link role *primaria, secundaria o negociable*

Configura la interfaz como una estación de enlace primaria, secundaria o negociable SDLC. El valor por omisión es primaria. La utilización de este mandato no afecta a la configuración de SRAM.

Notas:

1. Para DLSw, **negotiable** utiliza X'FF' (dirección de difusión) para el sondeo inicial.
Cuando se utiliza la dirección de difusión para negociar la función, el enlace utiliza una configuración SDLC por omisión.
Cuando **primary** es la función del enlace, éste realiza un sondeo inicial para una dirección específica.
2. Para APPN de punto a punto o negociable, se utiliza la dirección de difusión para el sondeo inicial. Para el multipunto primario, se utiliza la dirección específica.
3. Para SDLC conmutado, el dispositivo debe ser primario, de modo que **link role type** no es configurable para las interfaces de circuito de marcación SDLC.

link secondary-pause

Especifica el período de tiempo que la estación secundaria retrasará el envío del final del sondeo después de que se haya sondeado.

Notas:

1. Este valor debe ser menor que el tiempo de espera excedido de sondeo para la estación primaria.
2. Los valores mayores que 0 en enlaces multipunto pueden provocar tiempos de respuesta pobres.

Supervisión de interfaces SDLC

Valores válidos: De 0 a 25,5 segundos en incrementos de 0,1 segundo. Un valor de > 0 es más útil en enlaces de punto a punto TWS ya que permite que ambas direcciones envíen a la vez.

Valor por omisión: 0

link snrm *tiempo de espera excedido o reintento*

Para estaciones primarias, cambia dinámicamente la información de SNRM(E) siguiente sin afectar a la configuración de SRAM.

timeout

El tiempo que se ha de esperar una respuesta de Reconocimiento no numerado (UA) antes de retransmitir un SNRM(E).

retry El número de veces que se ha de retransmitir un SNRM(E) sin recibir una respuesta antes de abandonar.

Ejemplo:

```
set link snrm timeout
Enter SNRM response timeout [2.0]?
```

link type multipoint or point-to-point

Cambia dinámicamente un enlace multipunto o un enlace de punto a punto sin afectar a la configuración de SRAM.

Nota: Para SDLC conmutado, el enlace es siempre de punto a punto, de modo que **link type** no es configurable para las interfaces de circuito de marcación SDLC.

link xid/test *tiempo de espera excedido o reintento*

Para estaciones primarias, cambia dinámicamente la información de XID/PRUEBA siguiente sin afectar a la configuración de SRAM.

timeout

El período máximo de tiempo que se ha de esperar una respuesta de trama XID o TEST antes de retransmitir una trama de prueba.

retry El número máximo de veces que una trama XID o TEST se vuelve a enviar antes de dejarlo. Un 0 (cero) hace que el direccionador lo reintente indefinidamente.

Nota: Se pueden encontrar ejemplos y explicaciones de los parámetros siguientes en el capítulo de configuración de SDLC en la sección "Set" en la página 732.

station *dirección o nombre* **address**

Cambia la dirección SDLC de la estación.

station group-inclusion

Para estaciones secundarias SDLC, establezca si se ha de incluir esta estación en la lista de sondeo de grupo para este enlace. Para que esto sea efectivo, añada una dirección de sondeo de grupo secundario utilizando el mandato **set link group-poll**.

Ejemplo: `set station c1 group-inclusion yes`

station gp-addres-prim

Especifica la dirección de grupo que se ha de sondear. Una dirección específica no puede utilizarse también como dirección de grupo.

Supervisión de interfaces SDLC

Valores válidos: De X'00' a X'FE', donde X'00' indica que no se utiliza el sondeo de grupo

Valor por omisión: X'00'

station dirección o nombre max-packet

Tamaño máximo de paquete que esta estación puede recibir.

station dirección o nombre name

Nombre de la estación SDLC.

station protocol

Define si la estación se ejecuta como TWA o TWS.

Nota: TWS necesita hardware dúplex.

station dirección o nombre receive-window

Número máximo de tramas que el direccionador recibe antes de que sea necesario un reconocimiento.

station secondary poll pause

Especifica el período de tiempo que la estación secundaria retrasará el envío del final del sondeo después de que se haya sondeado.

Notas:

1. Este valor debe ser menor que el tiempo de espera excedido de sondeo para la estación primaria.
2. Los valores mayores que 0 en enlaces multipunto pueden provocar tiempos de respuesta pobres.

Valores válidos: De 0 a 25,5 segundos en incrementos de 0,1 segundo. Un valor mayor que 0 es más útil en enlaces de punto a punto TWS ya que permite que ambas direcciones envíen a la vez.

Valor por omisión: 0

station dirección o nombre transmit-window

Número máximo de tramas que el direccionador transmite antes de recibir una trama de respuesta.

Test

Transmite un número especificado de tramas TEST a la estación especificada y espera una respuesta. Utilice este mandato para probar la integridad de la conexión. Pulse cualquier tecla para cancelar la prueba.

Nota: Inhabilite la estación de enlace especificada antes de utilizar este mandato

Sintaxis:

test *station nombre o dirección númerotramas-a-enviar*
tamaño-trama

Ejemplo:

```
test station c1
Number of frames to send [1]? 5
Frame length [265]?
Starting echo test -- press any key to abort
5 frames sent, 5 frames received, 0 compare errors, 0 timeouts
```

Number of test frames to send

Número total de tramas que se han de enviar.

Frame length

Longitud de las tramas que se han de enviar. La longitud de las tramas no puede ser superior a la longitud máxima de trama para la estación especificada.

La prueba puede cancelarse anormalmente pulsando cualquier tecla.

Interfaces SDLC y mandato interface de GWCON

Aunque la interfaz SDLC tiene un proceso de consola con finalidad operativa, el 2216 también visualiza estadísticas completas para las interfaces instaladas cuando se utiliza el mandato **interface** en el entorno GWCON. (Para obtener más información sobre el mandato **interface**, consulte la sección “Capítulo 8. El proceso de operación/supervisión (GWCON - Talk 5) y sus mandatos” en la página 117.)

Estadísticas visualizadas para interfaces SDLC

Mediante la utilización del mandato **interface**, puede visualizar estadísticas para dispositivos SDLC sin entrar en el proceso de supervisión SDLC. Para hacerlo, entre el mandato **interface** y un número de interfaz en el indicador +.

+ **interface 12**

Este mandato lista las estadísticas en el formato siguiente:

Nt	Nt'	Interface	Slot-Port	Self-Test Passed	Self-Test Failed	Maintenance Failed
12	12	SDLC/0	Slot: 8 Port: 2	2	1	0
SDLC MAC/data-link on V.35/V.36 interface						
Adapter cable:		V.35 DTE				
V.24 circuit:		105 106 107 108 109				
Nicknames:		RTS CTS DSR DTR DCD				
PUB 41450:		CA CB CC CD CF				
State:		ON ON ON ON ON				
Line speed:		64.000 Kbps				
Last port reset:		1 hour, 20 minutes, 42 seconds ago				
Input frame errors:						
CRC error				0	alignment (byte length)	0
missed frame				182	too long (> 2062 bytes)	0
aborted frame				0	DMA/FIFO overrun	0
Output frame counters:						
DMA/FIFO underrun errors				0	Output aborts sent	0

Nt Indica el número de interfaz tal como lo ha asignado el software durante la configuración inicial.

Nt' Indica el número de interfaz tal como lo ha asignado el software durante la configuración inicial.

Nota: Para interfaces SDLC, el número de interfaz Nt' es siempre igual al número de interfaz Nt.

Slot Indica el número de ranura de la interfaz que ejecuta SDLC.

Port Indica el número de puerto de la interfaz que ejecuta SDLC.

Self-test passed

Indica el número total de veces que la interfaz SDLC ha pasado su autoprueba.

Supervisión de interfaces SDLC

Self-test failed

Indica el número total de veces que la interfaz SDLC no ha podido pasar su autoprueba.

Maintenance failed

Indica el número de anomalías de mantenimiento.

Los parámetros siguientes sólo se visualizan si hay un cable conectado. La información visualizada depende del cable que está conectado. Se visualizan diferentes parámetros con otros cables.

Adapter cable

Indica el tipo de cable de adaptador que está utilizando el conversor de nivel.

V.24 circuit

Indica los circuitos que se utilizan en V.24.

Nicknames

Indica las señales que se utilizan en el circuito V.24.

RS-232

Los nombres de circuitos EIA 232 (RS 232).

State Indica el estado de los circuitos, señales y asignaciones de patillas V.24 (ON u OFF).

Line speed (configured)

Indica la velocidad de línea configurada actualmente para la interfaz SDLC.

Last port reset

Indica cuánto tiempo hace que se restableció el puerto por última vez.

Input frame errors

Indica el tipo de error de trama de entrada (error CRC, demasiado corto, cancelado anormalmente, alineación, demasiado largo, desbordamiento DMA/FIFO) y el número total de errores que se han producido.

Output frame counters

Indica el número total de desbordamientos DMA/FIFO y de cancelaciones anormales de salida enviados para tramas de salida.

Missed frame

Cuando una trama llega al dispositivo y no hay ningún almacenamiento intermedio disponible, el hardware elimina la trama e incrementa el contador de tramas que faltan.

L & F bits not set

En interfaces serie, el hardware establece información de descriptor de entrada para las tramas que llegan. Si el almacenamiento intermedio puede aceptar toda la trama en la llegada, el hardware establece el último y el primer bit de la trama, lo que indica que el almacenamiento intermedio ha aceptado toda la trama. Si no se establece alguno de estos bits, se elimina el paquete, se incrementa el contador L & F bits not set y se borra el almacenamiento intermedio para reutilización.

Nota: No es probable que el contador L & F bits not set se vea afectado por el tráfico.

Capítulo 50. Utilización de la interfaz de red V.25bis

La interfaz V.25bis permite a los direccionadores establecer conexiones serie a través de líneas telefónicas conmutadas utilizando módems V.25bis. Este capítulo describe cómo utilizar la interfaz V.25bis. Incluye las secciones siguientes:

- “Antes de empezar”
- “Procedimientos de configuración”

Notas:

1. Puede asignar un nombre de destino a una **connection list** y asignar un número de destino a cada línea de la lista. Cuando se llama a ese nombre de destino, se intentan uno a uno los números de la lista hasta que se establece una conexión o se agota la lista.
2. V.25bis sólo está soportada en el adaptador EIA 232 de 8 puertos.

Antes de empezar

Antes de configurar V.25bis en el direccionador, asegúrese de que tiene lo siguiente:

- Módems V.25bis que soporten los mandatos síncronos V.25bis y la especificación 1988 ITU/CCITT V.25bis.
- Si el módem no detecta automáticamente el origen de la repuesta, debe:
 - Configurar el módem en un extremo del enlace para que origine llamadas.
 - Configurar el módem del otro extremo del enlace para que responda a las llamadas.
 - Configurar el módem en el extremo de respuesta para la respuesta automática.

Procedimientos de configuración

Esta sección describe cómo configurar el direccionador para V.25bis. Las tareas que es necesario realizar son:

1. Añadir direcciones V.25bis
2. Configurar los parámetros V.25bis
3. Añadir circuitos de marcación
4. Configurar los circuitos de marcación

Nota: Debe reiniciar el direccionador para que los cambios en la configuración de V.25bis surtan efecto.

Adición de direcciones V.25bis

Necesita añadir una dirección V.25bis para cada interfaz V.25bis local, así como para cada destino. La dirección V.25bis incluye:

- *Nombre de dirección.* El nombre de dirección es una descripción de la dirección. Puede utilizar cualquier serie de un máximo de 23 caracteres ASCII imprimibles.
- *Dirección de marcación de red.* Número de teléfono del puerto local o de destino. Puede entrar hasta 30 caracteres que estén en el formato válido del módem V.25bis conectado. Para obtener información adicional consulte el manual del módem.

Nota: El juego de caracteres válido para los números de teléfono tal como lo define CCITT y soportado por el IBM 2216 incluye:

- Los dígitos decimales del 0 al 9

Utilización de V.25 bis

- Dos puntos (:) — "Tono de espera"
- Signo de menor que (<) — "Pausa", utilizado para insertar un retardo fijo (dependiendo del módem) entre secuencias de dígitos. Por ejemplo, cuando se pasa a través de un PBX o un PTN.
- Signo de igual (=) — "Separador 3", que es "para uso nacional". (Consulte el manual del módem.)
- La letra P — "La marcación se ha de continuar en modalidad de pulsos". (No soportado por algunos módems.)
- La letra T — "La marcación se ha de continuar en modalidad DTMF". (No soportado por algunos módems.)

Para añadir una dirección V.25bis, entre el mandato **add v25-bis-address** en el indicador Config>. Por ejemplo:

```
Config>add v25-bis-address
Assign address name [1-23] chars []? remote-site-baltimore
Assign network dial address [1-30 digits] []? 19095551234
```

Configuración de la interfaz V.25bis

Esta sección explica cómo configurar la interfaz V.25bis. Para realizar la configuración, lleve a cabo lo siguiente:

1. Para configurar una interfaz de línea serie para V.25bis, establezca el protocolo de enlace de datos para la interfaz de línea serie. En el indicador Config>, utilice el mandato **set data-link v25bis**. Por ejemplo:

```
Config>set data-link v25bis
Interface Number [0]? 2
```

2. Visualice el indicador V.25bis Config> entrando el mandato **network** seguido del número de la interfaz. Por ejemplo:

```
Config>network 2
V.25bis Data Link Configuration
V25bis Config>
```

Puede utilizar el mandato **list devices** en el indicador Config> para visualizar una lista de números de interfaz configurados en el direccionador.

3. Utilice el mandato **set local-address** para especificar el nombre de dirección de red del puerto local. Debe entrar uno de los nombres de dirección que ha definido utilizando el mandato **add v25bis-address**. Por ejemplo:

```
V25bis Config>set local-address
Local network address name []? remote-site-baltimore
```

Nota: Debe reiniciar el direccionador para que los cambios en la configuración surtan efecto.

Parámetros opcionales de V.25bis

Los siguientes son los parámetros opcionales de V.25bis que puede establecer. Para ver una descripción completa de estos mandatos, consulte la sección "Mandatos de configuración V.25bis" en la página 755.

- Puede limitar el número de llamadas sucesivas a una dirección inaccesible o que rechaza estas llamadas. Para hacerlo, utilice los mandatos **set retries-no-answer** y **set timeout-no-answer**.
- El mandato **set disconnect-timeout** controla el período de tiempo que el direccionador espera para iniciar una llamada después de desactivar una señal de la llamada anterior.
- El mandato **set command-delay-timeout** especifica el período de tiempo que el direccionador espera para iniciar o responder a una llamada después de activar DTR.

- El mandato **set connect-timeout** especifica el número de segundos permitidos para establecer una llamada.
- El mandato **set duplex** especifica la modalidad de dúplex para la llamada.
- El mandato **set encoding** establece la codificación para la llamada.
- Cuando haya terminado de configurar la interfaz, puede utilizar el mandato **list** para visualizar la configuración.

Adición de circuitos de marcación

Los circuitos de marcación se correlacionan con las interfaces de línea serie V.25bis. Puede correlacionar múltiples circuitos de marcación con una interfaz de línea serie.

Para añadir un circuito de marcación, utilice el mandato **add device dial-circuit** en el indicador `Config>`. El software asigna un número de interfaz a cada circuito. Utilizará este número para configurar el circuito de marcación.

Ejemplo:

```
Config>add device dial-circuit
Adding device as interface 6
```

Nota: Los circuitos de marcación toman por omisión Point-to-Point Protocol (PPP). También puede establecer que el circuito de marcación utilice Frame Relay (FR) o SDLC.

Configuración de circuitos de marcación

Esta sección describe cómo configurar un circuito de marcación. Para ver una descripción completa de los mandatos de los circuitos de marcación, consulte la sección “Capítulo 54. Configuración y supervisión de circuitos de marcación” en la página 797.

Nota: Si el tipo de encapsulador es SDLC, el único parámetro de circuito de marcación que puede establecer es el número de red base.

Para configurar el circuito de marcación, lleve a cabo lo siguiente:

1. Visualice el indicador `Circuit Config>` entrando el mandato **network** seguido del número de interfaz del circuito de marcación. Puede utilizar el mandato **list devices** en el indicador `Config>` para visualizar una lista de los circuitos de marcación que ha añadido. Por ejemplo:

```
Config>network 6
Circuit configuration
Circuit Config>
```

2. Correlacione el circuito de marcación con una interfaz V.25bis. La red base es el número de interfaz V.25bis. Por ejemplo:

```
Circuit Config>set net
Base net for this circuit [0]? 0
```

3. Especifique el nombre de dirección del direccionador remoto al que se conectará el circuito de marcación. Debe utilizar uno de los nombres que ha definido utilizando el mandato **add v25-bis-address**. Por ejemplo:

```
Circuit Config>set destination
Assign destination address name []? newyork
```

4. Configure el circuito de marcación para que sólo inicie llamadas de salida, sólo acepte llamadas de entrada o que inicie y acepte llamadas.

Utilice el mandato **set calls**. Para evitar un conflicto si ambos extremos del enlace intentan establecer una llamada a la vez, configure el circuito de marcación en un extremo del enlace para que sólo acepte llamadas de

Utilización de V.25 bis

entrada y configure el circuito de marcación en el otro extremo del enlace para que sólo inicie llamadas de salida. Por ejemplo:

```
Circuit Config>set calls outbound  
Circuit Config>set calls inbound
```

Nota: Para las operaciones de Restauración de WAN u otra aplicación de marcación a petición, debe configurar el circuito para llamadas de entrada o de salida.

5. Especifique el período de tiempo de espera excedido para el circuito. Utilice el mandato **set idle**. Si no hay tráfico a través del circuito durante este período de tiempo especificado, el circuito de marcación queda en suspenso. Para configurar el circuito como un circuito dedicado, establezca el temporizador de desocupado en cero. Para configurar el circuito para que marque a petición, establezca el temporizador de desocupado en un valor distinto de cero. El rango va de 0 a 65535 y el valor por omisión es 60 segundos. Por ejemplo:

```
Circuit Config>set idle  
Idle timer (seconds, 0 means always active) [60]? 0
```

Nota: Para operaciones de Restauración de WAN o de Redireccionamiento de WAN debe establecer el tiempo de desocupado en 0.

6. Opcionalmente, puede retardar el tiempo entre el establecimiento de una llamada y el envío del paquete inicial. Utilice el mandato **set selftest-delay**. El establecimiento de un retardo de autopruueba puede evitar que se eliminen paquetes. Si los módems tardan un tiempo adicional en sincronizarse, ajuste este retardo. Por ejemplo:

```
Circuit Config>set selftest-delay  
Selftest delay(milli-seconds,0 means no delay) [150]?200
```

7. Establezca el nombre de dirección de entrada. Utilice el mandato **set inbound**. Sólo necesita utilizar este mandato si configura el circuito para llamadas de entrada y de salida y si la dirección de destino del direccionador es diferente de la dirección de destino que el direccionador remoto marca. Por ejemplo, los números pueden ser diferentes si uno de los direccionadores pasar a través de un intercambio PVX, internacional o inter-LATA. Por ejemplo:

```
Circuit Config>set inbound  
Assign destination inbound address name []? newyork
```

El nombre de dirección de entrada debe coincidir con uno de los nombres que ha definido utilizando el mandato **add v25-bis-address**.

8. Establezca la modalidad de dúplex utilizando el mandato **set duplex**.
9. Establezca la modalidad de codificación para el circuito utilizando el mandato **set encoding**.
10. Opcionalmente, puede entrar en el proceso de configuración para el protocolo de capa de enlace datos que está ejecutándose en el circuito de marcación (PPP o Frame Relay). Utilice el mandato **encapsulator**. Por ejemplo:

```
Circuit Config>encapsulator
```

Capítulo 51. Configuración y supervisión de la interfaz de red V.25bis

Este capítulo describe los mandatos de configuración y operativos de V.25bis y los mandatos GWCON. Incluye las secciones siguientes:

- “Acceso al proceso de configuración de interfaces”
- “Mandatos de configuración V.25bis”
- “Acceso al proceso de supervisión de interfaces” en la página 759
- “Mandatos de supervisión V.25bis” en la página 760
- “V.25bis y los mandatos GWCON” en la página 764

Acceso al proceso de configuración de interfaces

Utilice el procedimiento siguiente para acceder al proceso de configuración V.25bis.

1. En el indicador OPCON, entre el mandato **talk** y el PID para CONFIG. (Para ver los detalles de este mandato, consulte la sección ¿Qué es el proceso OPCON?.) Por ejemplo:

```
* talk 6
Config>
```

Después de entrar el mandato **talk 6**, se visualiza el indicador CONFIG (Config>) en la consola. Si no aparece el indicador cuando entre en **CONFIG**, pulse **Intro** de nuevo.

2. En el indicador CONFIG, entre el mandato **list devices** para visualizar los números de las interfaces de red para las que el direccionador está configurado actualmente.
3. Anote los números de interfaz.
4. Entre el mandato CONFIG **network** y el número de la interfaz que desea configurar. Por ejemplo:

```
Config> network 1
V.25bis Config>
```

Ahora, se visualiza el indicador de configuración V.25bis en la consola.

Mandatos de configuración V.25bis

La Tabla 97 resume y el resto de la sección explica los mandatos de configuración V.25bis. Estos mandatos le permiten visualizar, crear o modificar una configuración V.25bis. Entre los mandatos de configuración V.25bis en el indicador V.25bis Config>.

Tabla 97. Resumen de los mandatos de configuración V.25bis

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página 10.
List	Visualiza la configuración V.25bis.
Set	Establece la dirección local, los tiempos de espera excedidos de conexión, desconexión y sin respuesta, el número de reintentos después de no obtener respuesta, la modalidad de dúplex, el tiempo de espera excedido de retardo de mandatos y la codificación.

Mandatos de configuración V.25bis

Tabla 97. Resumen de los mandatos de configuración V.25bis (continuación)

Mandato	Función
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página 11.

List

Utilice el mandato **list** para visualizar la configuración actual de V.25bis.

Sintaxis:

list

Ejemplo:

```
list
      V.25bis Configuration

Duplex                = Full
Encoding              = NRZ
Local Network Address Name = v403
Local Network Address  = 15088982403

Non-Responding addresses:
Retries               = 1
Timeout               = 0 seconds

Call timeouts:
Command Delay         = 0 ms
Connect               = 60 seconds
Disconnect            = 2 seconds

Cable type            = V.35 DTE
Speed                  = 9600
```

Duplex

Visualiza la modalidad de dúplex para la interfaz una vez que se ha establecido la conexión de marcación.

Encoding

Visualiza el esquema de codificación de la transmisión para la interfaz, después de haber establecido la conexión de marcación. La codificación es NRZ (sin retorno a cero) o NRZI (inversión sin retorno a cero).

Local Network Address Name:

Visualiza el nombre de dirección de red del puerto local.

Local Network Address:

Visualiza la dirección de marcación de red del puerto local.

Non-responding addresses:

Retries

Número máximo de llamadas que el direccionador intenta realizar a una dirección que no responde, durante el período de tiempo de espera.

Timeout

Si el direccionador alcanza el número máximo de reintentos para una dirección que no responde, no intenta establecer la llamada hasta que ha caducado este tiempo. Este período de tiempo de espera excedido empieza cuando el direccionador intenta la primera llamada.

Call timeouts:

Número de tiempos de espera excedidos de llamada.

Command Delay

Período de tiempo, en milisegundos, que el direccionador espera para iniciar o responder a una llamada después de activar DTR (Terminal de datos preparado). Si establece este parámetro en 0, el direccionador espera que el módem responda al DTR con la señal CTS (Preparado para transmitir) antes de emitir mandatos.

Connect

Número de segundos permitidos para establecer una llamada. Si este parámetro se establece en 0, el módem controla el tiempo de espera excedido para el establecimiento de la conexión.

Disconnect

Después de que el direccionador desactive DTR espera este período de tiempo antes de iniciar más llamadas. Si establece este parámetro en 0, el direccionador espera que el módem responda a la desactivación de DTR desactivando CTS y DSR antes de iniciar la siguiente llamada.

Set

Utilice el mandato **set** para configurar las direcciones locales, los tiempos de espera excedidos y retardos para las llamadas, los reintentos y tiempos de espera excedidos para las direcciones que no responden y el tipo de cable HDLC.

Sintaxis:

```
set                command-delay timeout . . .  
                   connect-timeout . . .  
                   disconnect-timeout . . .  
                   duplex  
                   hdlc cable . . .  
                   hdlc encoding . . .  
                   hdlc speed . . .  
                   local-address . . .  
                   retries-no-answer . . .  
                   timeout-no-answer . . .
```

command-delay-timeout *núm. de milisegundos*

Después de que el direccionador active DTR (Terminal de datos preparado), espera este período de tiempo antes de iniciar o responder una llamada. Si establece este parámetro en 0, el direccionador espera que el módem responda al DTR con la señal CTS (Preparado para transmitir) antes de emitir mandatos. El rango va de 0 a 65535 milisegundos, y el valor por omisión es 0.

connect-timeout *núm. de segundos*

Establece el número de segundos permitidos para establecer una llamada. El rango es de 0 a 65535 segundos y el valor por omisión es 60. Si establece este parámetro en 0, el módem controla el tiempo de espera excedido de la conexión. Inicialmente, debe establecer este parámetro en 0 y, a continuación, utilizar el suceso ELS V25B.027 para averiguar lo que se

Mandatos de configuración V.25bis

tarda en establecer las conexiones con los diversos destinos. Después, puede establecer este parámetro en un número levemente superior al tiempo de conexión más largo.

Nota: Normalmente, la regulación estatal limita a los fabricantes de módems a una longitud máxima para la configuración de la llamada. Este valor es meramente una optimización, aunque para la interoperación con algunas DSU puede ser necesario cambiar este parámetro.

disconnect-timeout *núm. de segundos*

Especifica el período de tiempo, en segundos, que el direccionador espera después de desactivar DTR antes de iniciar más llamadas. El rango es de 0 a 65535 segundos y el valor por omisión es 2. Si establece este parámetro en 0, el direccionador espera a que el módem responda a la desactivación de DTR desactivando CTS y DSR antes de iniciar la siguiente llamada.

duplex

Especifica el tipo de dúplex de la línea.

Cuando se configura dúplex, la señal de módem RTS permanece activada después de haberse establecido la conexión de marcación.

Cuando se configura semi-dúplex, el direccionador activa RTS cuando es el momento de transmitir y espera que el módem active CTS. Después de activar CTS, el direccionador transmite paquetes de datos y, después, desactiva RTS cuando el direccionador ha terminado de transmitir para permitir que el dispositivo similar responda.

Sólo configure semi-dúplex cuando utilice la interfaz V.25bis para manejar SDLC conmutado y el módem conectado necesite la modalidad de funcionamiento de semi-dúplex.

Notas:

1. Debe establecerse en dúplex para los circuitos PPP o Frame Relay.
2. Si configura semi-dúplex para una interfaz V.25bis de un adaptador EIA-232E de 8 puertos, debe configurar la velocidad de línea utilizando el mandato **set hdlc speed**.

Valores válidos: dúplex o semi-dúplex

Valor por omisión: dúplex

hdlc cable *rs232 dte*

Especifica el tipo de cable conectado a esta interfaz. El establecimiento de este parámetro le permite ver el tipo de cable cuando entra el mandato **interface** en el indicador GWCON (+) y cuando entra el mandato **statistics** en el indicador de supervisión V.25bis>. Este parámetro no afecta al funcionamiento del direccionador.

hdlc encoding

Establece el esquema de codificación de la transmisión HDLC como NRZ (sin retorno a cero) o NRZI (inversión sin retorno a cero). La mayoría de configuraciones utilizan NRZ. La codificación configurada se utiliza para la conexión de extremo a extremo.

Nota: Aunque puede configurar NRZI, el intercambio entre el DTE y el módem (tal como se describe en la recomendación de CCITT, V.25bis) utiliza NRZ como el esquema de codificación.

Mandatos de configuración V.25bis

Valores válidos: NRZ o NRZI

Valor por omisión: NRZ

hdlc speed

Especifica la velocidad de línea para esta interfaz. El establecimiento de este parámetro le permite ver la velocidad de línea cuando entra el mandato `interface` en el indicador GWCON (+) y cuando entra el mandato `statistics` en el indicador de supervisión V.25bis>. El rango es de 2400 a 64 000 bps. El valor por omisión es 9600 bps.

Nota: Este mandato no afecta a la velocidad de línea real, pero establece la velocidad de algunos protocolos como, por ejemplo, IPX, utilizada al calcular los parámetros de coste de direccionamiento para los circuitos de marcación correlacionados con la interfaz V.25bis.

local-address *nombre de dirección*

Especifica el nombre de dirección de red del puerto local. Este nombre de dirección debe coincidir con uno de los nombres que haya definido en `Config>` utilizando el mandato **add v25-bis-address**.

Ejemplo: `set local-address line-1-local`

retries-no-answer *valor*

Algunos proveedores de servicio telefónico imponen restricciones en los dispositivos de rellamada automática para limitar el número de llamadas sucesivas a una dirección a la que no se puede acceder o que rechaza estas llamadas. Este parámetro especifica el número máximo de llamadas que el direccionador intenta realizar a una dirección que no responde durante el período de tiempo de espera excedido. El rango es de 0 a 10 y el valor por omisión es 1.

Nota: La normativa gubernamental también puede imponer límites a los fabricantes de módems que reemplazaría este parámetro.

timeout-no-answer *núm. de segundos*

Después de que el direccionador alcance el número máximo de **retries-no-answer** para una dirección que no responde, no inicia más llamadas para esta dirección hasta que este tiempo ha caducado. El período de tiempo de espera empieza cuando el direccionador intenta la primera llamada a una dirección. El rango es de 0 a 65535 segundos y el valor por omisión es 0. Si establece este parámetro en 0, el módem controla el período de tiempo de espera.

Acceso al proceso de supervisión de interfaces

Para acceder al proceso de supervisión de interfaces para V.25bis, entre el mandato siguiente en el indicador GWCON (+):

+ **network** *número*

Donde *número* es el número de línea serie V.25bis. No puede acceder directamente al proceso de supervisión V.25bis para los circuitos de marcación, pero puede supervisar los circuitos de marcación que están correlacionados con la interfaz de línea serie.

Nota: Las interfaces V.25bis también tienen mensajes de resolución de problemas ELS que puede utilizar para supervisar la actividad relacionada con V.25bis.

Mandatos de configuración V.25bis

Consulte la publicación *IBM Nways Guía de mensajes del sistema para el registro cronológico de sucesos* para ver más detalles.

Mandatos de supervisión V.25bis

Esta sección resume y explica los mandatos operativos V.25bis. Estos mandatos le permiten ver las llamadas, circuitos, parámetros y estadísticas de las interfaces V.25bis.

Entre los mandatos de supervisión V.25bis en el indicador V.25bis>. La Tabla 98 muestra los mandatos.

Tabla 98. Resumen de los mandatos de supervisión V.25bis

Mandato de supervisión	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado "Cómo obtener ayuda" en la página 10.
Calls	Lista el número de conexiones completadas e intentadas que se han realizado para cada circuito de marcación correlacionado con esta interfaz desde la última vez que se han restablecido las estadísticas del direccionador.
Circuits	Muestra el estado de todos los circuitos configurados en la interfaz V.25bis.
Parameters	Visualiza los parámetros actuales para la interfaz V.25bis. (Este mandato es similar al mandato V.25bis Config> list.)
Statistics	Visualiza las estadísticas actuales para la interfaz V.25bis.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página 11.

Calls

Utilice el mandato **calls** para listar el número de conexiones completadas e intentadas realizadas para cada circuito de marcación correlacionado con esta interfaz desde la última vez que se han restablecido las estadísticas del direccionador.

Sintaxis:

calls

Ejemplo:

```
calls
Net Interface Site Name           In   Out  Rfsd  Blckd
1   PPP/0     v403                2    0    0     0
Unmapped connection indications:  0
```

Net Número del circuito de marcación correlacionado con esta interfaz.

Interface

Tipo de interfaz y su número de instancia.

Site Name

Nombre de dirección de red del circuito de marcación.

In Número de conexiones de entrada aceptadas para este circuito de marcación.

- Out** Número de conexiones completadas iniciadas por este circuito de marcación.
- Rfsd** Número de conexiones iniciadas por este circuito de marcación que la red o el puerto de destino remoto han rechazado.
- Blckd** Número de intentos de conexión que el direccionador ha bloqueado. El direccionador bloquea los intentos de conexión si ya se utiliza el puerto local, se ha alcanzado el número máximo de reintentos para una dirección que no responde o un módem no responde.
- Unmapped connection indications:**
Número de intentos de conexión que el direccionador ha rechazado porque no había ningún circuito de marcación habilitado que estuviese configurado para aceptar las llamadas de entrada.

Circuits

El mandato **circuits** muestra el estado de todos los circuitos de marcación configurados en el puerto V.25bis.

Sintaxis:

circuits

Ejemplo:

```

circuit
Net Interface  MAC/Data-Link  State      Reason      Duration
2  PPP/0       Point to Point  Avail      Rmt Disc    1:02:25
    
```

Net Número del circuito de marcación correlacionado con esta interfaz

Interface

Tipo de interfaz y su número de instancia.

MAC/DataLink

Tipo de protocolo de enlace de datos configurado para este circuito.

State Estado actual del circuito de marcación:

- Up - conectado actualmente
- Available - no conectado actualmente, pero disponible
- Disabled - el circuito de marcación estaba inhabilitado
- Down - no se ha podido conectar debido a un circuito de marcación ocupado o a que el protocolo de capa de enlace está desactivado

Reason

Razón del estado actual:

- nnn_Data - (donde nnn es el nombre de un protocolo) el circuito está activado porque un protocolo tenía datos para enviar.
- Remote Disconnect - el circuito está desactivado o disponible porque el destino remoto ha desconectado la llamada.
- Operator Request - el circuito está disponible porque un mandato de supervisión ha desconectado la última llamada.
- Inbound - el circuito está activado porque el circuito ha respondido a una llamada de entrada.
- Restoral - el circuito está activado debido a una operación de Restauración de WAN.
- Self Test - el circuito se ha configurado como estático (idle time=0) y se ha conectado satisfactoriamente una vez se ha habilitado.

Duration

Período de tiempo que el circuito ha estado en el estado actual.

Mandatos operativos V.25bis

Parameters

Utilice el mandato **parameters** para visualizar la configuración actual de la línea serie V.25bis. Observe que se trata de la misma información visualizada en el mandato V.25bis Config> list.

Sintaxis:

parameters

Ejemplo:

```
parameters
V.25bis port Parameters

Local Network Address Name    = v402
Local Network Address        = 15088982402

Non-Responding addresses:
Retries                      = 1
Timeout                      = 0 seconds

Call timeouts:
Command Delay                = 0 ms
Connect                      = 0 seconds
Disconnect                   = 0 seconds
```

Local Network Address Name:

Nombre de dirección de red del puerto local.

Local Network Address:

Dirección de marcación de red del puerto local.

Non-responding addresses:

Retries

Número máximo de llamadas que el direccionador intenta realizar a una dirección que no responde, durante el período de tiempo de espera.

Timeout

Si el direccionador alcanza el número máximo de reintentos para una dirección que no responde, no intenta establecer la llamada hasta que ha caducado este tiempo. El período de tiempo de espera empieza cuando el direccionador intenta la primera llamada a una dirección.

Call timeouts:

Command Delay

Período de tiempo, en milisegundos, que el direccionador espera para iniciar o responder a una llamada después de activar DTR (Terminal de datos preparado). Si establece este parámetro en 0, el direccionador espera que el módem responda al DTR con la señal CTS (Preparado para transmitir) antes de emitir mandatos.

Connect

Número de segundos permitidos para establecer una llamada. Si este parámetro se establece en 0, el módem controla el tiempo de espera excedido para el establecimiento de la conexión.

Disconnect

Después de que el direccionador desactive DTR espera este período de tiempo antes de iniciar más llamadas. Si establece este

parámetro en 0, el direccionador espera que el módem responda a la desactivación de DTR desactivando CTS y DSR antes de iniciar la siguiente llamada.

Statistics

Utilice el mandato **statistics** para visualizar las estadísticas actuales para esta interfaz V.25bis.

Sintaxis:

statistics

Ejemplo:

```
statistics
    V.25bis port Statistics
```

```
Adapter cable:          RS-232 DTE
```

```
Nicknames:  RTS CTS DSR DTR DCD RI
RS-232      CA CB CC CD CF CE
State:      OFF OFF OFF OFF OFF OFF
```

```
Line speed:          4800
Last port reset:    24 seconds ago
```

```
Input frame errors:
  CRC error          0 alignment (byte length) 0
  missed frame      0 too long (> 2182 bytes) 0
  aborted frame     0 DMA/FIFO overrun        0
  L & F bits not set 0
Output frame counters:
DMA/FIFO underrun errors      0 Output aborts sent      0
```

Adapter cable:

Tipo de cable de adaptador que se utiliza.

Nicknames:

Nombres comunes para los circuitos.

RS-232

Nombres EIA 232 (también conocido como RS-232) para los circuitos.

State: Estado actual de los circuitos: ON, OFF o "---," que significa que el estado no está definido para este tipo de interfaz.

Line speed:

La velocidad de reloj de transmisión (aproximada).

Last port reset:

Período de tiempo desde que se ha restablecido el puerto.

Input frame errors:

CRC error

Número de paquetes recibidos que contenían errores de suma de comprobación y como consecuencia de ello se han eliminado.

Alignment (byte length)

Número de paquetes recibidos cuya longitud no era un múltiplo par de 8 bits y como consecuencia de ello se han eliminado.

Mandatos operativos V.25bis

Missed Frame

Cuando una trama llega al dispositivo y no hay ningún almacenamiento intermedio disponible, el hardware elimina la trama e incrementa el contador de tramas que faltan.

too long (> nnnn bytes)

Número de paquetes recibidos mayores que el tamaño de trama configurado (nnnn) y como resultado de ello se han eliminado.

aborted frame

Número de paquetes recibidos que se han cancelado anormalmente por el emisor o por un error de línea.

DMA/FIFO overrun

El número de veces que la tarjeta de interfaz serie no ha podido enviar datos con la suficiente rapidez a la memoria de almacenamiento intermedio de paquetes del sistema para recibir paquetes de la red.

L & F bits not set

En interfaces serie, el hardware establece información de descriptor de entrada para las tramas que llegan. Si el almacenamiento intermedio puede aceptar la trama completa en la llegada, el hardware establece el último y el primer bit de la trama, indicando que el almacenamiento intermedio ha aceptado toda la trama. Si no se establece alguno de estos bits, se elimina el paquete, se incrementa el contador L & F bits not set y se borra el almacenamiento intermedio para reutilización.

Nota: No es probable que el contador L & F bits not set se vea afectado por el tráfico.

Output frame counters:

DMA/FIFO underrun errors

Número de veces que la tarjeta de interfaz serie no ha podido recuperar datos con la suficiente rapidez de la memoria de almacenamiento intermedio de paquetes del sistema para transmitir paquetes a la red.

Output aborts sent

Número de transmisiones que se han cancelado anormalmente como petición del software de nivel superior.

V.25bis y los mandatos GWCON

Aunque V.25bis tiene su propio proceso de supervisión, el direccionador también visualiza información de configuración y estadísticas completas para los dispositivos y circuitos cuando se utilizan los mandatos `interface`, `statistics` y `error` desde el entorno GWCON. También puede utilizar el mandato `test` de GWCPM para probar los DCE y los circuitos.

Nota: La emisión del mandato `test` para la interfaz serie V.25bis hace que se desactive la llamada actual y se vuelva a marcar.

Para obtener más información sobre el mandato GWCON, consulte la sección "Capítulo 8. El proceso de operación/supervisión (GWCON - Talk 5) y sus mandatos" en la página 117.

Estadísticas para las interfaces V.25bis y circuitos de marcación

Utilice el mandato **interface** en el indicador GWCON (+) para visualizar las estadísticas para las interfaces de línea serie y los circuitos de marcación V.25bis.

Para visualizar las estadísticas siguientes para una interfaz de línea serie V.25bis, utilice el mandato **interface** seguido del *número de interfaz* de la interfaz de línea serie V.25bis.

Ejemplo: interface 10

```

                                Self-Test  Self-Test  Maintenance
                                Passed     Failed     Failed
10 10  V.25/0      Slot: 4  Port: 0      1         0         0
V.25bis Base Net MAC/data-link on EIA 232E/V.24 interface

Adapter cable:                RS-232 DTE

V.24 circuit: 105 106 107 108 109 125
Nicknames:    RTS CTS DSR DTR DCD RI
RS-232:       CA  CB  CC  CD  CF  CE
State:        OFF OFF OFF ON  OFF OFF

Line speed:           ~ 19.200 Kbps
Last port reset:     55 minutes, 1 second ago

Input frame errors:
CRC error                6  alignment (byte length)      0
missed frame            1  too long (> 2054 bytes)     0
aborted frame          34  DMA/FIFO overrun            0
Output frame counters:
DMA/FIFO underrun errors 0  Output aborts sent          0

```

Para visualizar las estadísticas siguientes para un circuito de marcación, utilice el mandato **interface** seguido del *número de interfaz* del circuito de marcación.

Ejemplo:

interface 29

```

                                Self-Test  Self-Test  Maintenance
                                Passed     Failed     Failed
29 10  PPP/20      2         1         0
Point to Point MAC/data-link on V.25bis Dial Circuit interface

```

La lista siguiente describe la salida para las interfaces de línea serie y los circuitos de marcación.

Nt El número de interfaz de la línea serie o el número de interfaz del circuito de marcación.

Nt' Si "Nt" es un circuito de marcación, se trata del número de interfaz de la interfaz de línea serie V.25bis con la que se correlaciona el circuito de marcación.

Interface

El tipo de interfaz y su número de instancia.

Slot El numero de ranura de la interfaz que ejecuta V.25bis.

Port El número de puerto de la interfaz que ejecuta V.25bis.

Self-Test Passed

Número de autopruebas que han sido satisfactorias.

Self-Test Failed

Número de autopruebas que han fallado.

Mandatos operativos V.25bis

Maintenance: Failed

Número de anomalías de mantenimiento.

Adapter cable:

Tipo de cable del adaptador que se utiliza.

V.24 circuit:

Números de circuito tal como los identifican las especificaciones de V.24.

RS-232

Nombres EIA 232 (también conocido como RS-232) para los circuitos.

State Estado actual de los circuitos (ON u OFF).

Line speed

La velocidad de reloj de transmisión (aproximada).

Last port reset

Período de tiempo desde que se ha restablecido el puerto.

Input frame errors:

CRC error

Número de paquetes recibidos que contenían errores de suma de comprobación y como consecuencia de ello se han eliminado.

Alignment (byte length)

Número de paquetes recibidos cuya longitud no era un múltiplo par de 8 bits y como consecuencia de ello se han eliminado.

Missed Frame

Cuando una trama llega al dispositivo y no hay ningún almacenamiento intermedio disponible, el hardware elimina la trama e incrementa el contador de tramas que faltan.

too long (> nnnn bytes)

Número de paquetes recibidos mayores que el tamaño de trama configurado y como resultado de ello se han eliminado.

DMA/FIFO overrun

El número de veces que la tarjeta de interfaz serie no ha podido enviar datos con la suficiente rapidez a la memoria de almacenamiento intermedio de paquetes del sistema para recibir paquetes de la red.

L & F bits not set

En interfaces serie, el hardware establece información de descriptor de entrada para las tramas que llegan. Si el almacenamiento intermedio puede aceptar la trama completa en la llegada, el hardware establece el último y el primer bit de la trama, indicando que el almacenamiento intermedio ha aceptado toda la trama. Si no se establece alguno de estos bits, se elimina el paquete, se incrementa el contador L & F bits not set y se borra el almacenamiento intermedio para reutilización.

Nota: No es probable que el contador L & F bits not set se vea afectado por el tráfico.

aborted frame

Número de paquetes recibidos que se han cancelado anormalmente por el emisor o por un error de línea.

Output frame counters:

DMA/FIFO underrun errors

Número de veces que la tarjeta de interfaz serie no ha podido recuperar datos con la suficiente rapidez de la memoria de almacenamiento intermedio de paquetes del sistema para transmitir paquetes a la red.

Output aborts sent

Número de transmisiones que se han cancelado anormalmente como petición del software de nivel superior.

Mandatos operativos V.25bis

Capítulo 52. Utilización de la interfaz RDSI

Importante

Los LIC originales de un solo puerto 2216 RDSI T1 y E1 (IBM PN 11J7466 ó 78H6147 y 11J7465 ó 78H6148 respectivamente), no soportan la asignación de direcciones MAC para clientes DIAL. Esta asignación sólo es necesaria para los clientes que deseen utilizar los protocolos NetBIOS y/o SNA nativamente en el entorno Acceso remoto a la LAN DIAL. Todas las demás funciones RDSI y las funciones DIAL (por ejemplo, Dial-in IP e IPX) funcionarán correctamente sin ninguna actualización. Los nuevos LIC de un solo puerto RDSI T1 y E1 soportan la asignación de direcciones MAC para clientes DIAL y todas las funciones DIAL. Los clientes con los LIC RDSI originales que deseen utilizar las funciones DIAL de NetBIOS y/o SNA deben ponerse en contacto con el representante de servicio IBM para actualizar a los nuevos LIC.

Este capítulo describe las interfaces Integrated Services Digital Network (RDSI) en el IBM 2216. Incluye las secciones siguientes:

- “Visión general de RDSI”
- “Códigos de causa RDSI” en la página 772
- “Configuraciones RDSI de ejemplo” en la página 774
- “T1/E1 canalizado” en la página 775
- “Requisitos y restricciones para interfaces RDSI” en la página 776
- “Antes de empezar” en la página 776
- “Procedimientos de configuración” en la página 777.
- “Variante de conmutador I.431” en la página 781

Visión general de RDSI

El software de interfaz RDSI le permite establecer conexiones RDSI entre direccionadores o desde un usuario de marcación de entrada a un direccionador. Puede configurar la interfaz para que actúe como un enlace dedicado o para inicie y acepte conexiones de circuito conmutado, a petición, automáticamente desde el reinicio o por un mandato del operador.

I.430, I.431 y T1/E1 canalizados no están conmutados. Son conexiones de tipo de línea alquilada permanente.

Adaptadores e interfaces RDSI

El IBM 2216 soporta los adaptadores RDSI-PRI siguientes:

- RDSI-PRI E1 de 1 puerto
- RDSI-PRI T1/J1 de 1 puerto
- RDSI-PRI E1 de 4 puertos
- RDSI-PRI T1/J1 de 4 puertos
- RDSI-PRI E1 de 8 puertos
- RDSI-PRI T1/J1 de 8 puertos

Los adaptadores PRI/canalizados tienen una CSU/DSU integrada, por lo que no es necesario ninguna CSU/DSU externa.

Utilización de RDSI

Nota: Si está actualizando desde BRI a PRI en talk 6, debe borrar primero las configuraciones de RDSI y de marcación, después activar PRI y configurar PRI.

- El adaptador PRI no soporta el multipunto.
- El adaptador PRI proporciona soporte de T1/J1 y E1.
 - T1/J1 soporta veintitrés canales B de 64 kbps y un canal D de 64 kbps.
 - E1 soporta treinta canales B de 64 kbps y un canal D de 64 kbps.
- El adaptador PRI proporciona el soporte de ID de línea ampliada (LID).

Circuitos de marcación

Hay cuatro tipos de circuitos de marcación:

- Circuitos estáticos (o enlace)

Notas:

1. I.430, I.431 y T1/E1 canalizado son conexiones de línea alquilada y por lo tanto no realizan marcaciones.
 2. RDSI considera que el tráfico X.25 a través del canal D es un circuito estático. Sin embargo, podría configurar el circuito X.25 como un PVC o SVC utilizando el mandato **encapsulator** bajo la configuración del circuito de marcación.
- Los circuitos conmutados que marcan a petición y quedan en suspenso después de un tiempo de desocupado especificado
 - Los circuitos de restauración de WAN que sólo se utilizan cuando falla una línea alquilada primaria asignada
 - Los circuitos de marcación de entrada se utilizan para proporcionar a los clientes remotos el acceso a los recursos de la red.

Cuando se establecen puentes en una interfaz de marcación a petición, se recomienda inhabilitar el árbol de expansión para esta interfaz y crear filtros MAC para filtrar todo el tráfico no deseado. (Los filtros MAC eliminarían todas las tramas que no estuviesen destinadas a direcciones MAC específicas.) Esto evita que el circuito de marcación permanezca conectado debido a tráfico no deseado.

Nota: No es necesario que añada ningún filtro MAC cuando ejecute el tráfico BAN en una interfaz de marcación a petición FR. El software BAN siempre realiza el filtrado, de modo que el único tráfico de puente que hará que el circuito de marcación a petición no quede en suspenso será el tráfico cuya dirección MAC de destino coincide con la dirección MAC del DLCI BAN.

Añada un circuito de marcación para cada posible destino. Puede correlacionar múltiples circuitos de marcación con una interfaz RDSI. Cada circuito de marcación es una red de línea serie normal, que ejecuta Point-to-Point Protocol (PPP), Frame Relay o X.25 (sólo para canales D). Estos protocolos están configurados para funcionar a través de circuitos de marcación.

Nota: Puede asignar un nombre de destino a una **connection list** (añada la dirección RDSI) y asignar un número de destino a cada línea de la lista. Cuando se llama a ese nombre de destino, se intentan uno a uno los números de la lista hasta que se establece una conexión o se agota la lista.

Los protocolos redireccionables y las características de puente y direccionamiento no pueden comunicarse directamente con una interfaz RDSI. Es necesario

configurar estos protocolos para ejecutarlos en circuitos de marcación. Esta implementación soporta los protocolos y características siguientes para los circuitos de marcación RDSI:

- APPN
- Banyan VINES
- DECnet
- DLSw
- IP
- IPX
- IPv6
- AppleTalk 2
- Puenteado (SRB, STP, SR-TB y SRT)
- Reserva de ancho de banda
- Restauración de WAN
- DIALS

Direccionamiento

Para realizar una llamada RDSI, especifique el número de teléfono de destino. Para identificarse a sí mismo en el conmutador, debe especificar su propio número de teléfono. Para RDSI, los números de teléfono se llaman direcciones de marcación de red y, por conveniencia, se les dan nombres llamados nombres de dirección de red que representan el número de teléfono.

Cuando se configura una interfaz RDSI, se añaden las direcciones de cada posible destino así como el número de teléfono propio, al que se llama dirección de red local. Cuando se configura un circuito de marcación, la dirección de red local se obtiene de la configuración de interfaz física y se establece una dirección de destino para el circuito.

Exceso de suscripciones y contención de circuitos

Una interfaz RDSI PRI T1/J1 puede soportar un máximo de 23 llamadas activas y una interfaz RDSI PRI E1 puede soportar un máximo de 30 llamadas activas. Puede haber más circuitos de marcación configurados en una interfaz RDSI que las llamadas activas soportadas. Esto se denomina exceso de suscripciones. Si un circuito de marcación intenta una llamada cuando la interfaz RDSI tiene todas las llamadas activas, hay dos posibilidades: 1) Si el circuito de marcación tiene una prioridad superior que el circuito de marcación con una llamada activa, ésta terminará para el circuito de marcación de prioridad inferior y se intentará una llamada para el circuito de marcación de prioridad superior. 2) Si el circuito de marcación no tiene una prioridad superior a ningún circuito de marcación con llamadas activas, no se realiza ninguna llamada. El direccionador eliminará los paquetes enviados por los protocolos de los circuitos de marcación que no pueden conectarse a su destino RDSI.

Nota: No hay ninguna contención de circuitos cuando se ejecuta X.25 a través del canal D porque el canal D siempre está disponible para la conexión X.25.

Consulte la sección "Set" en la página 801 para obtener más información acerca de la prioridad.

Control del coste a través de circuitos a petición

Para los protocolos, los circuitos de marcación a petición siempre parece que están en estado Activo. La mayoría de protocolos envían información periódica de direccionamiento que podría hacer que el direccionador realizase una marcación de

Utilización de RDSI

salida cada vez que se enviase información de direccionamiento a través de circuitos de marcación a petición. Para limitar las actualizaciones periódicas de direccionamiento, configure IP y OSE para que sólo utilicen rutas estáticas e inhabilite los protocolos de direccionamiento (RIP, OSPF) a través de los circuitos de marcación. Si utiliza IPX, configure rutas y servicios estáticos e inhabilite los protocolos de direccionamiento (RIP, SAP) a través de los circuitos de marcación. Otra opción es configurar intervalos de actualización de RIP y SAP de baja frecuencia, aunque esto no impide que RIP y SAP difundan los cambios de información de direccionamiento a medida que se producen. También debe habilitar el filtro de Mantener activo IPX, que impide que los paquetes de mantener activo y de serialización activen continuamente el enlace de marcación a petición.

ID y LIDS del llamador

Si el servicio RDSI proporciona el servicio ANI o CallerID (CLID) proporcionando el Número de la parte llamador (CPN) en el mensaje de configuración RDSI, puede utilizarlo para emparejar los circuitos de marcación con el llamador adecuado. De lo contrario, debe utilizar un protocolo de identificación de línea de propiedad (LID) o proporcionar circuitos que sean "ANY INBOUND".

El protocolo LID utiliza el destino de entrada en la configuración del circuito de marcación y el LID recibido para emparejar el circuito de marcación llamador con el circuito de marcación receptor. El protocolo LID es un protocolo de identificación breve iniciado por el llamador y contestado por el receptor. Si el llamador no proporciona el mensaje LID, el receptor puede rechazar la llamada, si el circuito de marcación any_inbound no está configurado. Los intercambios de LID se producen en el canal B.

Cuando se conectan dos rutas que no soportan id lógicos (LIDS), puede suprimir el intercambio de LID utilizando la opción de configuración bajo el circuito de marcación individual.

```
config> set lid_used no
```

En la parte de la entrada, si lid_used=no, se completa la llamada y el IBM 2216 no espera que llegue el LID en el canal B. En su lugar, el IBM 2216 intenta utilizar el callerID recibido. Si no hay ninguna coincidencia de callerID, el IBM 2216 comprueba si hay un circuito de marcación any_inbound disponible. Si no hay ningún circuito any_inbound disponible, se rechaza la llamada.

En la parte de la salida, se inicia la autoprueba PPP/FR inmediatamente, después se asigna el canal B.

Códigos de causa RDSI

Esta implementación de RDSI especifica un código de causa que impedirá al direccionador que intente establecer una conexión a través de una interfaz RDSI. Si la aplicación reintenta, el direccionador vuelve a intentar establecer una conexión a través de esta interfaz y lo conseguirá si se ha corregido el problema original. Si durante el reintento el direccionador encuentra el mismo código de causa, la aplicación no volverá a intentar más el proceso de conexión a través de esta interfaz.

Interpretaciones de los códigos de causa:

1. Si cause0 no es "0x5" pase por alto el código de causa.
2. Si cause0 es "0x5" consulte cause1. Si el bit de orden superior (más significativo) de cause1 es 0N, establézcalo en OFF.

3. Convierta el resultado a decimal y consulte el significado en la tabla siguiente, que se ha extraído de la publicación *ITU-T Recommendation Q.850*.

Tabla 99. Códigos de causa RDSI Q.931

Código	Causa
1	Desasignado (número no asignado)
2	No hay ninguna ruta para la red de tránsito especificada
3	No hay ninguna ruta para el destino
6	Canal no aceptable
7	Llamada adjudicada y se está entregando en un canal establecido
16	Borrado normal de llamada
17	Usuario ocupado
18	No responde ningún usuario
19	No hay respuesta del usuario (usuario avisado)
21	Llamada rechazada
22	Número cambiado
26	Borrado de usuario no seleccionado
27	Destino fuera de servicio
28	Formato de número no válido (dirección incompleta)
29	Recurso rechazado
30	Respuesta a STATUS ENQUIRY
31	Normal, no especificado
34	No hay circuito/canal disponible
38	Red fuera de servicio
41	Anomalía temporal
42	Congestión de equipo de conmutación
43	Información de acceso desechada
44	Circuito/canal pedido no disponible
47	Recurso no disponible, no especificado
49	Calidad de los servicios no disponible
50	Recurso pedido no suscrito
57	Posibilidad de transporte no autorizada
58	Posibilidad de transporte no disponible actualmente
63	Servicio u opción no disponible, no especificado
65	Posibilidad de transporte no implementada
66	Tipo de canal no implementado
69	Recurso pedido no implementado
70	Sólo está disponible la posibilidad de transporte de información digital restringida
79	Servicio u opción no implementado, no especificado
81	Valor de referencia de llamada no válida
82	El canal identificado no existe
83	Existe una llamada suspendida, pero no esta identidad de llamada
84	Identidad de llamada en uso

Utilización de RDSI

Tabla 99. Códigos de causa RDSI Q.931 (continuación)

Código	Causa
85	No hay ninguna llamada suspendida
86	Se ha borrado la llamada que tenía esta identidad de llamada
88	Destino incompatible
91	Selección de red de tránsito no válida
95	Mensaje no válido, no especificado
96	Falta elemento de información obligatorio
97	Tipo de mensaje no existente o no implementado
98	Mensaje no compatible con estado de llamada o tipo de mensaje no existente o no implementado
99	Elemento de información no existente o no implementado
100	Contenido de elemento de información no válido
101	Mensaje no compatible con estado de llamada
102	Recuperación de caducidad del temporizador
111	Error de protocolo, no especificado
127	Gestión entre redes, no especificado

Configuraciones RDSI de ejemplo

Los temas siguientes muestran varias configuraciones RDSI típicas.

Configuración Frame Relay a través de RDSI

La Figura 50 le muestra cómo puede conectar una red Frame Relay a través de una red RDSI. En esta configuración, se establece el enlace de datos en los circuitos de marcación para Frame Relay.

Nota: Los circuitos de marcación toman por omisión Point-to-Point Protocol (PPP). Para cambiar el protocolo a Frame Relay, entre **set data-link fr** en el indicador **Config>**. Una conexión sólo se podrá utilizar si el enlace de datos de ambos extremos coincide (por ejemplo, FR a FR o PPP a PPP).

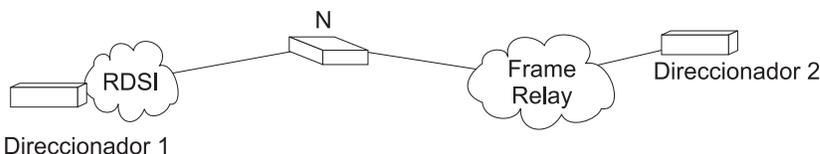


Figura 50. Configuración Frame Relay a través de RDSI

Nota: N podría ser un RDSI TA conectado al conmutador FR o una tarjeta RDSI de un conmutador FR.

Configuración de Restauración de WAN

La Figura 51 en la página 775 le muestra cómo puede utilizar una conexión RDSI como reserva de un enlace WAN dedicado que ha fallado (Restauración de WAN). En este ejemplo, normalmente el Direccionador A utiliza el enlace WAN para comunicarse con el Direccionador B. Si esta conexión falla, el enlace de marcación RDSI vuelve a conectar los dos direccionadores. Cuando se recupera el enlace

WAN, el enlace secundario se desconecta automáticamente. Para obtener más información sobre cómo configurar el direccionador para la Restauración de WAN, consulte la sección Utilización de restauración de WAN de la publicación *Utilización y configuración de las características*.

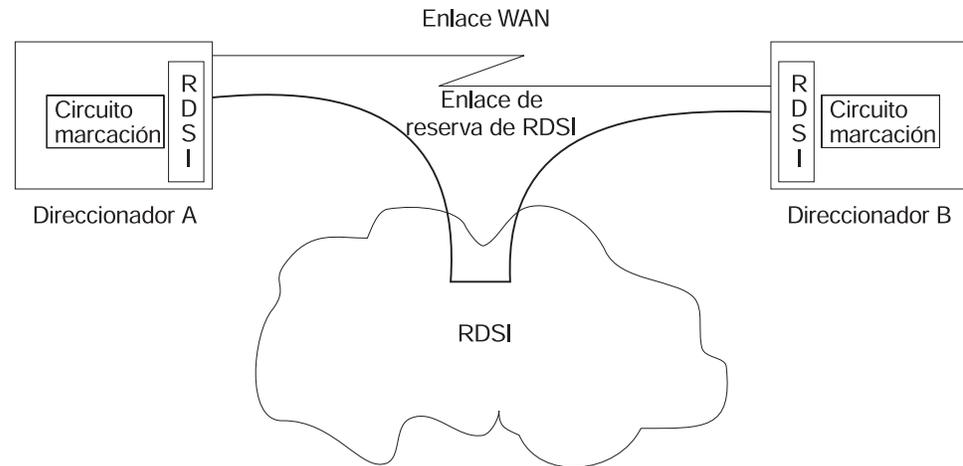


Figura 51. Utilización de RDSI para la Restauración de WAN

Para la Restauración de WAN, sólo pueden utilizarse los circuitos configurados para PPP como enlace secundario. Para el Redireccionamiento de WAN, pueden utilizarse un circuito de marcación PPP o un circuito de marcación FR como enlace alternativo.

T1/E1 canalizado

Cuando está configurado como canalizado, el adaptador canalizado/PRI le permite obtener el soporte de T1/J1/E1 fraccional/canalizado. Puede tener canales de 56 kbps o N*64 kbps. Esto le permitirá multiplexar múltiples conexiones de líneas alquiladas (por ejemplo: utilizando V.35 a 56 kbps) en una conexión física.

Para configurar un adaptador T1 o E1 primario como canalizado:

1. Seleccione "Canalizado" como la variante de conmutador para la interfaz RDSI.
2. Configure los períodos de tiempo que se han de utilizar para esta interfaz RDSI cuando configure el circuito de marcación. Consulte la sección "Set" en la página 801 para obtener más información.

Ejemplo de configuración de una interfaz T1 canalizada:

```
Config>n 6
RDSI Config>set switch chan
RDSI Config>list
```

RDSI Configuration

```
Maximum frame size in bytes      = 2048
Switch Variant/Service Type     = Channelized
Available Timeslots: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
```

```
Config>n 7
Circuit config: 7>set net 6
Circuit config: 7>set timeslot 2 3 4 24
Circuit config: 7>list
```

Utilización de RDSI

Base net	= 6
Idle character	= 7E
Bandwidth	= 64 Kbps
Timeslot	= 2 3 4 24

Nota: Si fuese un circuito E1, los períodos de tiempo disponibles serían del 1 al 31.

Requisitos y restricciones para interfaces RDSI

Conmutadores/Servicios soportados

La Interfaz de velocidad primaria (PRI) RDSI soporta los conmutadores/servicios siguientes:

Nombres de conmutadores	Mandato válido
AT&T 5ESS (Norteamérica)	5ESS
AT&T 4ESS (Norteamérica)	4ESS
Australia (AUSTEL)	AUSPRI
INS-Net 1500 (Japón, NTT)	INSPRI
National RDSI 2 (Norteamérica)	USNI2
NET 5 (RDSI europeo, ETSI)	NET5
Northern Telecom DMS (DMSPRI)	DMSPRI
Native I.431	I431 (Consulte la sección “Variante de conmutador I.431” en la página 781.)
T1/E1 canalizado	CHANNELIZED

Restricciones de interfaz RDSI

- No puede arrancar ni volver el direccionador a través de una interfaz RDSI.
- Excepto por BRI, que le permite utilizar el canal D para los datos de paquete X.25, no puede utilizar el canal D para el tráfico de datos. Normalmente el canal D sólo se utiliza para configurar y desactivar las conexiones del canal B.

Requisitos de configuración de circuitos de marcación

Necesita considerar lo siguiente al configurar PPP o Frame Relay con RDSI:

- La interfaz RDSI no impondrá los contadores de retardo de transmisión establecidos en las configuraciones PPP.
- No habilite pseudo-serial-ethernet en el circuito de marcación.

Antes de empezar

Antes de configurar RDSI, necesita la siguiente información:

- El número de teléfono del puerto RDSI local.
- Los números de teléfono de destino, incluyendo cualquier extensión telefónica.
- El tipo de conmutador al que está conectada la interfaz RDSI. Consulte la sección “Conmutadores/Servicios soportados” para ver la lista de conmutadores.

Nota: Puede que sean necesarios parámetros adicionales como, por ejemplo, TEI y SPID en base al Tipo de conmutador y al proveedor de servicio.

Procedimientos de configuración

Esta sección describe cómo configurar la interfaz RDSI y sus circuitos de marcación asociados. Específicamente, las tareas que es necesario realizar son:

1. Añadir direcciones RDSI
2. Configurar los parámetros RDSI
3. Configurar la Interfaz RDSI
4. Añadir circuitos de marcación
5. Configurar los circuitos de marcación

Nota: Debe reiniciar el direccionador para que los cambios en la configuración surtan efecto.

Adición de direcciones RDSI

Necesita añadir una dirección RDSI para cada interfaz RDSI, así como para cada destino. La dirección RDSI incluye:

- *Nombre de dirección.* El nombre de dirección es una descripción de la dirección. Puede utilizar cualquier serie de un máximo de 23 caracteres ASCII imprimibles.
- *Dirección de marcación de red.* Número de teléfono del puerto local o de destino. Puede entrar hasta 25 números, así como 6 caracteres incluyendo la puntuación. El direccionador sólo utiliza los números.
- *Dirección de submarcación de red.* Opcional. Es una parte adicional del número de teléfono como, por ejemplo, una extensión, que se interpreta cuando la interfaz se conecta a un PBX. Puede entrar hasta 20 números, así como 11 espacios adicionales y puntuación. El direccionador sólo utiliza los números.

Para añadir una dirección RDSI, entre el mandato **add isdn-address** en el indicador Config>. Por ejemplo:

```
Config>add isdn-address
Assign address name [23] chars []? baltimore
Assign network dial address [1-15 digits] []? 1-555-0983
Assign network subdial address [1-20 digits] []? 23
```

Para ver una lista de las direcciones RDSI, entre **list isdn-address** en el indicador Config>.

Para suprimir una dirección RDSI de la lista, entre el mandato **delete isdn-address** en el indicador Config>.

Configuración de parámetros RDSI

Acceda al indicador RDSI Config>. Para acceder al indicador RDSI Config>, entre el mandato **network** seguido por el número de la interfaz RDSI en el indicador Config>. Por ejemplo:

```
Config>network 3
ISDN user configuration
ISDN Config>
```

Puede utilizar el mandato **list devices** en el indicador Config> para visualizar una lista de números de interfaz configurados en el direccionador. Consulte la sección "Mandatos de configuración RDSI" en la página 783 para obtener más información acerca de los mandatos de configuración.

1. Especifique el tipo de conmutador/dispositivo al que esta interfaz RDSI está conectada.

Utilización de RDSI

Utilice el mandato **set switch-variant** para especificar el tipo de conmutador al que esta interfaz RDSI está conectada. Consulte la sección “Conmutadores/Servicios soportados” en la página 776 para ver la lista de conmutadores/dispositivos. Por ejemplo:

```
ISDN Config>set switch net5
```

Se trata del tipo de software que se ejecuta en el conmutador (por ejemplo, DMS100 significa la ejecución del software de cliente DMS100).

2. Especifique el nombre de dirección de red del puerto local.

Utilice el mandato **set local-address-name** para especificar el nombre de dirección de red del puerto local. Debe utilizar uno de los nombres de dirección que ha definido utilizando el mandato **add isdn-address**. Por ejemplo:

```
ISDN Config>: set local-address-name  
Assign local address name []? baltimore
```

Nota: Esto es lo que se enviará al campo Número de la parte llamadora del mensaje de configuración RDSI.

3. Establezca el número de directorio del puerto local.
4. Para establecer el tamaño de trama, utilice el mandato **set framesize**. Por ejemplo:

```
ISDN Config>set framesize  
Framesize in bytes (1024/2048/4096/8192) [1024]? 2048
```

Nota: Si elige un tamaño de trama de 1024, PPP no funcionará a través del circuito de marcación RDSI, ya que el tamaño mínimo de trama para PPP es 1500.

Para obtener más información acerca del establecimiento del tamaño de trama RDSI, consulte la sección “Set” en la página 784.

Parámetros opcionales de RDSI

Esta sección describe los parámetros opcionales de RDSI que puede establecer. Para ver una descripción completa de estos mandatos consulte la sección “Mandatos de configuración RDSI” en la página 783.

- Para todos los conmutadores RDSI, excepto INSPRI, puede configurar el límite de número de llamadas para una dirección. Utilice el mandato **set retries-call-address** para establecer el número de llamadas para un destino que no responde. Utilice el mandato **set timeout-call-address** para establecer el período de tiempo que se ha de esperar antes de intentar de nuevo la llamada.

Cuando haya terminado de configurar la interfaz RDSI, puede utilizar el mandato **list** para visualizar la configuración.

Configuración de la interfaz RDSI

Para la PRI RDSI, necesita configurar T1/J1 o E1 para cada adaptador, dependiendo del mismo.

Interfaz PRI T1/J1

Especifique los siguientes parámetros T1/J1:

1. Para la interfaz PRI T1/J1, la reducción de línea especifica la atenuación de la señal transmitida por el puerto T1 del direccionador. Especifique 1bo (reducción de línea) basándose en la información proporcionada por el proveedor del servicio.
 - a= -00.0 dB
 - b= -07.5 dB

```
c= -15.0 dB
d= -22.5 dB
```

Por ejemplo:

```
set int lbo a
```

2. Especifique el código, B8ZS o AMI. B8ZS es el valor por omisión. El proveedor del servicio proporciona esta información.

Por ejemplo:

```
set int code AMI
```

3. Especifique ZBTSI- Zero Byte Time Slot Inversion, ENABLED o DISABLED. El valor por omisión es DISABLED. El proveedor del servicio proporciona esta información.

Por ejemplo:

```
set int ZBTSI enabled
```

4. Especifique esf-data-link. Seleccione una de las siguientes opciones basándose en la suscripción del servicio:

ANSI-T1.403 ANSI-IDLE AT&T-IDLE

El valor por omisión es ANSI-T1.403

Por ejemplo:

```
set int esf-data-link ansi-idle
```

Interfaz PRI E1

Para la interfaz E1 PRI, especifique los parámetros siguientes:

1. Especifique el código, HDB3 o AMI. HDB3 es el valor por omisión. El proveedor del servicio proporciona esta información.

Por ejemplo:

```
set int code HDB3
```

2. Especifique crc4, ENABLED o DISABLED. El valor por omisión es ENABLED. El proveedor del servicio proporciona esta información.

Por ejemplo:

```
set int crc4 enabled
```

Adición de circuitos de marcación

Los circuitos de marcación se correlacionan con interfaces RDSI. Puede correlacionar múltiples circuitos de marcación con una interfaz RDSI.

Para añadir un circuito de marcación, entre el mandato **add device dial-circuit** en el indicador Config>. El software asigna un número de interfaz a cada circuito.

Utilizará este número para configurar el circuito de marcación. Por ejemplo:

```
Config>add device dial-circuit
Enter the number of PPP Dial Circuit interfaces [1]?
Adding device as interface 6
Base net for the circuits(s) [0]?
```

El número de circuitos de marcación que pueden configurarse depende del número total de parámetros que se hayan de configurar y el tamaño del archivo de configuración resultante.

Nota: Los circuitos de marcación toman por omisión Point-to-Point Protocol (PPP). Para cambiar el protocolo de circuito de marcación a Frame Relay, entre el mandato **set data-link fr** en el indicador Config>. No están soportados otros tipos de enlace de datos (X.25, SDLC y SRLY) a través de RDSI.

Configuración de circuitos de marcación

Esta sección describe cómo configurar un circuito de marcación.

1. Visualice el indicador `Circuit Config>` entrando el mandato **network** seguido del número de interfaz del circuito de marcación. Puede entrar el mandato **list devices** en el indicador `Config>` para visualizar una lista de los números de interfaces configurados en el direccionador. Por ejemplo:

```
Config> network 6
Circuit configuration
Circuit Config>
```

2. Correlacione el circuito de marcación con una interfaz RDSI. Utilice el mandato **set net**. La red base es el número de interfaz RDSI. (Sólo es necesario si cambia la red base.) Por ejemplo:

```
Circuit Config> set net
Base net for this circuit [0]? 3
```

Nota: Si el tipo de enlace de datos del circuito de marcación es X.25 o la variante de conmutador de red base es I.43x o canalizado, no se aplican los pasos siguientes (3-11 en la página 781).

3. Especifique el nombre de dirección del direccionador remoto al que se conectará el circuito de marcación. Debe utilizar uno de los nombres que ha definido utilizando el mandato **add isdn-address**. Por ejemplo:

```
Circuit Config> set destination
Assign destination address name []? baltimore
```

4. Configure el circuito de marcación para que sólo inicie llamadas de salida, sólo acepte llamadas de entrada o que inicie y acepte llamadas.

Utilice el mandato **set calls**. Por ejemplo:

```
Circuit Config> set calls outbound
Circuit Config> set calls inbound
Circuit Config> set calls both
```

Nota:

5. Especifique el período de tiempo de espera excedido para el circuito. Utilice el mandato **set idle**. Si no hay tráfico a través del circuito durante este período de tiempo especificado, el circuito de marcación queda en suspenso. Para configurar el circuito como un circuito dedicado, establezca el temporizador de desocupado en cero. Para configurar el circuito para que marque a petición, establezca el temporizador de desocupado en un valor distinto de cero. El rango va de 0 a 65535 y el valor por omisión es 60 segundos. Por ejemplo:

```
Circuit Config> set idle
Idle timer (seconds, 0 means always active) [0]? 0
```

Nota: La restauración/redireccionamiento de WAN debe arreglarse.

6. Opcionalmente, puede proporcionar un nombre LID para enviar (en lugar del LID por omisión, que es el nombre de destino) especificando una dirección de salida de LID.

Cuando se configuran más de un circuito entre dos direccionadores (circuitos paralelos), debe haber una manera de conocer qué circuito de marcación los conecta. Para esta finalidad, se envía un `lid_out_addr` desde el direccionador a un extremo (el llamador). El direccionador receptor debe tener una dirección de destino de entrada que coincida con el `lid_out_dirección` del direccionador emisor para que los circuitos de marcación se conecten. El `lid_out_addr` debe ser un nombre de dirección que se haya añadido previamente utilizando "ADD ISDN-ADDRESS" en el indicador **config>**.

```
Circuit Config> set lid_out_addr router2
```

- Opcionalmente, puede establecer la prioridad relativa de los circuitos de marcación.

El campo de prioridad permite que un circuito tenga preferencia sobre otro cuando no hay canales disponibles. Si se realiza una llamada de salida y se están utilizando todos los canales, se comprueba la prioridad del circuito de marcación que la pide con todos los circuitos de marcación activos. Si hay uno cuya prioridad es inferior a esta, se desconecta este circuito y se realiza una llamada para el circuito de marcación de prioridad superior.

Nota: Sólo se desactivarán los circuitos de marcación a petición.

Consulte la sección “Set” en la página 801 para obtener más información acerca de la prioridad.

```
Circuit Config> set priority 1
```

- Opcionalmente, puede retardar el tiempo entre el establecimiento de una llamada y el envío del paquete inicial. Utilice el mandato **set selftest-delay**. Algunos conmutadores RDSI empiezan a enviar datos antes de recibir una señal que indique un establecimiento completo del circuito en el destino. El establecimiento de un retardo de autoprueba puede evitar que se eliminen paquetes. Por ejemplo:

```
Circuit Config> set selftest-delay
Selftest delay(milli-seconds,0 means no delay) [150]?200
```

- Establezca el nombre de dirección de entrada.

Utilice el mandato **set inbound**. Este mandato sólo es para circuitos de entrada. Por ejemplo:

```
Circuit Config> set inbound
Assign destination inbound address name [ ]? newyork
```

El número de destino de entrada se utiliza para emparejar el LID de entrada o CallerID con el circuito de marcación. Si hay una coincidencia, este circuito de marcación tiene la llamada.

- Opcionalmente, puede entrar en el proceso de configuración para el protocolo de capa de enlace datos que está ejecutándose en el circuito de marcación (PPP o Frame Relay).

Utilice el mandato **encapsulator**. Por ejemplo:

```
Circuit Config> encapsulator
```

- Opcionalmente, puede utilizar el mandato **set bandwidth** para establecer la velocidad de línea a la que se ha de realizar la llamada (56 kbps o 64 kbps). Esto proporciona un control por llamada de las interfaces RDSI. Por ejemplo:

```
Circuit Config> set bandwidth 56kbps
```

Variante de conmutador I.431

Codifique la variante de conmutador como I.431 cuando ejecute una línea alquilada a través de RDSI PRI (sólo T1/J1).

Soporte de I.431 nativo

Cuando configure el soporte de I.431 nativo, sólo debe utilizar un circuito de marcación. Debe conectarse a la red base. I.431 sólo se ejecuta en el adaptador RDSI PRI T1. La velocidad se fija en 1,5 Mbps.

Utilización de RDSI

Nota: Los adaptadores RDSI PRI multipuerto no soportan la variante de conmutador I.431. Para utilizar toda una línea PRI, seleccione la variante canalizada y asigne todos los períodos de tiempo a un circuito de marcación.

Ejemplo: Red RDSI base

```
Config> n 5
ISDN Config> set sw i431
ISDN Config> list all
      ISDN Configuration

Maximum frame size in bytes = 2048
Switch Variant               = I431 PRI
```

Ejemplo: Circuito de marcación

```
Config> n 6
Circuit config: 6>set net 5
Circuit config: 6>list all

Base net                    = 5
```

Capítulo 53. Configuración y supervisión de la interfaz RDSI

Este capítulo describe los mandatos RDSI y los mandatos GWCON. Incluye las secciones siguientes:

- “Mandatos de configuración RDSI”
- “Acceso al proceso de supervisión de interfaces” en la página 789
- “Mandatos de supervisión RDSI” en la página 789
- “RDSI y los mandatos GWCON” en la página 793
- “Soporte para la reconfiguración dinámica de RDSI” en la página 795

Notas:

1. Las interfaces RDSI tienen mensajes ELS y códigos de causa que puede utilizar para supervisar la actividad relacionada con RDSI. Consulte la publicación *Guía de mensajes del sistema para el registro cronológico de sucesos*
2. Están disponibles los subsistemas ELS de RDSI, Q931, CEME, LAPD y DIAL.

Mandatos de configuración RDSI

La Tabla 100 describe los mandatos de configuración RDSI y las secciones siguientes explican los mandatos. Entre estos mandatos en el indicador ISDN Config>.

Tabla 100. Resumen de los mandatos de configuración RDSI

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página 10.
Block-calls	Bloquea las llamadas de entrada de un llamador específico.
Disable	Sólo es válido para BRI. Inhabilita la detección de la Fuente de alimentación 1.
Enable	Sólo es válido para BRI. Habilita la detección de la Fuente de alimentación 1.
List	Visualiza la configuración de RDSI.
Remove	Elimina las entradas DNO de la configuración RDSI.
Set	Establece el tamaño de trama, la dirección local, los tiempos de espera excedido sin repuesta, el número de reintentos después de que no haya respuesta, el tipo de conmutador RDSI, los números de directorio, SPIDS y el TEI.
Cause Code	Detiene los intentos de proceso para establecer una conexión a través de una interfaz.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página 11.

Block-Calls

Utilice los mandatos **block-calls** para bloquear las llamadas de entrada. Los números de llamador que se han de bloquear se han de añadir a la lista de autenticación. El número máximo de llamadas de llamador bloqueadas es de 16 por interfaz.

El bloqueo de llamada puede utilizarse para:

- Una llamada no solicitada que se está recibiendo constantemente.

Mandatos de configuración RDSI

- En la activación/prueba de la red, ya que es necesario pasar por alto algunas llamadas.

Sintaxis:

```
block-calls          add
                       list
                       remove
```

Add Añade el número de un llamador que se ha de bloquear.

List Lista los números de llamadores que se han de bloquear.

Remove

Elimina el número de un llamador de la lista que se ha de bloquear.

List

El mandato **list** visualiza la configuración RDSI actual.

Sintaxis:

```
list
_
```

Ejemplo: list

```

                                     ISDN Configuration
Local Network Address Name           = local2216
Local Network Address:Subaddress     = 2542216:

  Maximum frame size in bytes        = 2048
Outbound call address Timeout        = 180 Retries = 2
Switch Variant                       = NT DMS-250
DN0 (Directory Number 0)             = 2542216
No circuit address accounting information being kept.

T1/J1 Interface Parameters:

LBO                                   = 00.0 dB
Code                                  = B8ZS
ZBTSI                                 = Disabled
ESF-Data-Link                         = ANSI-IDLE
```

Remove

El mandato **remove** le permite eliminar las entradas DN0 o DN1 que ha establecido previamente con el mandato **set DN0** o **set DN1**.

Sintaxis:

```
remove                DN0-entry...
```

Ejemplo:

```
remove DN0
```

Set

El mandato **set** configura el tamaño de trama, las direcciones y los tiempos de espera excedidos. También especifica la variante de conmutador y el número de TEI. Para PRI, el identificador de punto final de terminal (TEI) siempre es cero (0).

Sintaxis:

```
set                   framesize...
                       interface
```

Mandatos de configuración RDSI

interface frame
_local-address-name...
RAI-type¹
_retries-call-address...
switch-variant...
dn0...

framesize 1024, 2048, 4096 ó 8192

Establece el tamaño de parte de capa de la red de tramas transmitidas y recibidas en la interfaz RDSI. No se incluyen las cabeceras de enlace de datos y de capa MAC. Debe establecer el tamaño de trama RDSI para que sea mayor o igual al tamaño de trama configurado para los circuitos de marcación que utilizan la interfaz RDSI.

Para las interfaces de circuito de marcación PPP, puede cambiar la MRU de PPP utilizando el mandato **set lcp options**. El tamaño de trama RDSI debe incluir suficientes bytes para la MRU de PPP y la cabecera PPP.

Nota: Si elige un tamaño de trama de 1024, PPP no funcionará a través del circuito de marcación RDSI, ya que el tamaño mínimo de trama para PPP es 1500.

Para interfaces de circuito de marcación FR, puede cambiar el tamaño de trama utilizando el mandato **set framesize**. El tamaño de trama RDSI debe ser mayor o igual al tamaño de trama FR.

Si el tamaño de trama de un circuito de marcación es mayor que el tamaño de trama del circuito RDSI, el tamaño de trama del circuito de marcación se reduce cuando se reinicializa el direccionador.

Ejemplo:

```
set framesize  
Framesize in bytes (1024/2048/4096/8192) [1024]? 2048
```

interface

Sólo para PRI. Establece los valores de los parámetros de interfaz siguientes para las líneas T1 y E1.

Para T1 PRI:

lbo La atenuación de la señal transmitida por el puerto T1 del direccionador. Esta información la proporciona el proveedor del servicio.

Valores válidos:

a= -00,0 dB
b= -07,5 dB
c= -15,0 dB
d= -22,5 dB

Valor por omisión: a

code Esta información la proporciona el proveedor del servicio.

Valores válidos: B8ZS o AMI

1. PRI only

2. Sólo canalizado

Mandatos de configuración RDSI

Valores por omisión: B8ZS

interface frame

Las opciones son D4 o ESF. Esto especifica un formato multitrama T1. Sólo se soporta ESF para la modalidad no canalizada. La trama de la interfaz se configura bajo el menú de red RDSI base.

Ejemplo:

```
set interface frame
Circuit config: 10>set interface frame
```

ZBTSI Inversión de período de tiempo de byte cero. Esta información la proporciona el proveedor del servicio.

Valores válidos: Habilitado o Inhabilitado

Valor por omisión: Inhabilitado

esf-data-link

La suscripción del servicio. Esta información la proporciona el proveedor del servicio.

Valores válidos:

ANSI-T1.403
ANSI-IDLE
AT&T-IDLE

Valor por omisión: ANSI-T1.403

RAI-type

Las opciones son ANSI o japonés. Esto especifica el método de indicar a RAI de la línea T1 cuándo se utiliza el sistema de tramas D4. ANSI RAI se indica por un valor 0 en el bit 2 de todos los canales. RAI japonés se indica por el valor 1 en la posición del bit S de la trama 12. El tipo de RAI se configura bajo el menú de red RDSI base.

Para E1 PRI:

code Esta información la proporciona el proveedor del servicio.

Valores válidos: HDB3 o AMI

Valor por omisión: HDB3

crc4 Especifica si el puerto E1 del direccionador transmitirá las palabras de código crc4 y las comprobará en las tramas recibidas. Esta información la proporciona el proveedor del servicio.

Valores válidos: Habilitado o Inhabilitado

Valor por omisión: Habilitado

local-address-name *nombre de dirección*

Se trata del nombre de dirección de red de la interfaz RDSI local. Este nombre de dirección debe coincidir con uno de los nombres que ha definido en el indicador Config> utilizando el mandato **add isdn-address**.

Valores válidos: Cualquier dirección válida

Valor por omisión: Ninguna

Ejemplo:

```
set local-address-name
Assign local address name []? line-1-local
```

retries-call-address *valor*

Algunos proveedores de servicio telefónico imponen restricciones en los dispositivos de rellamada automática para limitar el número de llamadas sucesivas a una dirección a la que no se puede acceder o que rechaza estas llamadas. **Retries-call-address** especifica el número máximo de llamadas que el direccionador intenta realizar a la vez. Si se establece **retries-call-address** en 0, el direccionador activa todos los circuitos a la vez.

Si establece la variante de conmutador en INS64, no puede cambiar el valor por omisión de **retries-call-address**. Se fija en 2.

Valores válidos: De 0 a 30

Valor por omisión: 23 (2 para BRI)

switch-variant *4ess, 5ess, auspri usni2 o ins1500 or dms250 o channel*

Especifica el modelo de conmutador al que está conectada esta interfaz RDSI. Puede elegir variantes de conmutador/tipo de servicio para la interfaz de velocidad primaria RDSI en las listas siguientes.

Valores válidos de Interfaz de velocidad primaria RDSI (PRI)/canalizada T1/E1:

- AT&T 5ESS (Norteamérica)
- AT&T 4ESS (Norteamérica)
- Australia (AUSTEL)
- INS-Pri (Japón, NTT)
- National ISDN 2 (Norteamérica)
- NET 5 (RDSI europeo, ETSI)
- Northern Telecom 250 (DMSPRI)
- I.431 nativo (sólo es válido para T1)
- T1/E1 canalizado

Valor por omisión: DMSPRI

dn0 *número de directorio 0*

Para aceptar llamadas de entrada **DN0** debe coincidir con la dirección de marcación de red (número de teléfono) que ha configurado utilizando el mandato **set local-address-name**. Si DN0 no está configurado, no se efectúa ninguna comprobación y se aceptarán todas las llamadas. Si el conmutador no proporciona el número de la parte llamada en el mensaje de configuración de entrada, DN0 no debe configurarse. Consulte en la página 787 para obtener información adicional.

Ejemplo:

```
set dn0
Enter DN0 (Directory-Number-0) [ ]? 5088981234
```

Nota: Esto se aplica a todas las variantes de conmutador RDSI de velocidad básica:

- DN0 y DN1 se utilizan para verificar que la llamada de entrada se está entregando al destino RDSI correcto.
- Si el número de destino (Número de parte llamada) de la llamada RDSI que se entrega no coincide con DN0 ni DN1, se rechaza la llamada.
- Si el usuario desea evitar la comprobación de la verificación del destino, no configure DN0 ni DN1. Si la línea RDSI que suministra sólo tiene un DN y el usuario desea utilizar la verificación del destino, debe configurar DN0. No configure DN1 a menos que se suministre la línea RDSI para dos DN.

Mandatos de configuración RDSI

- Cuando configure los SPID y los TEI, asegúrese siempre de configurar los primeros SPID (SPID[0]) y TEI (TEI[0]). Provocará errores si tiene configurado un SPID[1] o TEI[1] sin configurar SPID[0] o TEI[0].

Cause Code

Utilice el mandato **Cause Code** para impedir que el direccionador vuelva a intentar establecer una conexión a través de la interfaz RDSI cuando recibe una respuesta “especificada” (valor válido). Entre estos mandatos en el indicador Cause Config>.

Sintaxis:

cause code ? (Ayuda)
_add
_list
_remove
_exit

Tabla 101. Resumen de los mandatos de códigos de causa de RDSI

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página 10.
Add	Añade entradas de códigos de causa a la configuración RDSI.
List	Visualiza las listas de códigos de causa para la configuración RDSI.
Remove	Elimina entradas de códigos de causa de la configuración RDSI.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página 11.

Add Utilice el mandato **add** para añadir un código de causa a una configuración RDSI.

Valores válidos: Cualquier valor hexadecimal entre 01 y FF

Valor por omisión: Ninguno

Sintaxis: cause code add *valor*

Ejemplo: add FF

List Utilice el mandato **list** para mostrar la lista de códigos de causa de una configuración RDSI.

Sintaxis: cause code list

Remove

Utilice el mandato **remove** para eliminar un código de causa de una configuración RDSI.

Valores válidos: Cualquier valor hexadecimal entre 01 y FF

Valor por omisión: Ninguno

Sintaxis: cause code remove *valor*

Ejemplo: remove FF

Mandatos de supervisión RDSI

remove

Add Añade el número de un llamador que se ha de bloquear.

List Lista los números de llamadores que se han de bloquear.

Remove

Elimina el número de un llamador de la lista que se ha de bloquear.

Calls

Utilice el mandato **calls** para listar el número de conexiones completadas e intentadas realizadas para cada circuito de marcación correlacionado con esta interfaz desde la última vez que se han restablecido las estadísticas del direccionador.

Sintaxis:

calls

Ejemplo:

```
calls
Net Interface Site Name      In   Out   Rfsd  Blckd
 4   PPP/1   v403                2    0     0     0
```

Unmapped connection indications: 0

Net Número del circuito de marcación correlacionado con esta interfaz.

Interface

Tipo de interfaz y su número de instancia.

Site Name

Nombre de dirección de red del circuito de marcación.

In Conexiones de entrada aceptadas para este circuito de marcación.

Out Conexiones completadas iniciadas por este circuito de marcación.

Rfsd Conexiones iniciadas por este circuito de marcación que la red o el puerto de destino remoto han rechazado.

Blckd Intentos de conexión que el direccionador ha bloqueado. The router blocks connection attempts if all available channels are in use, if the maximum retries are used up and the router is waiting for the timer to count down, or if Layer 1 is up, but Layer 2 is down.

Unmapped connection indications:

Intentos de conexión que el direccionador ha rechazado porque no habían circuitos de marcación disponibles que estuviesen configurados para aceptar llamadas de entrada.

Channels

El mandato **channels** lista las estadísticas para un canal de la Interfaz de velocidad primaria RDSI.

Sintaxis:

channels

Circuits

El mandato **circuits** muestra el estado de los circuitos de marcación configurados en la interfaz RDSI que están en estado "Up" o "Available".

Sintaxis:**circuits****Ejemplo:**

```

circuit
Net Interface MAC/Data-Link State Reason Duration
4 PPP/1 Point to Point Up B1 SelfTest 91:24:03
5 PPP/2 Point to Point Up B2 Inbound 91:24:00

```

Net Número del circuito de marcación correlacionado con esta interfaz

Interface

Tipo de interfaz y su número de instancia.

MAC/Data-Link

Tipo de protocolo de enlace de datos configurado para este circuito de marcación.

State Estado actual del circuito de marcación:

Up Conectado actualmente.

Available

No conectado actualmente, pero disponible.

Disabled

Circuito de marcación inhabilitado.

Down No se ha podido conectar debido a un circuito de marcación ocupado o porque el protocolo de capa de enlace está desactivado.

Reason

Razón del estado actual:

nnn_Data

(Donde nnn es el nombre de un protocolo.) El circuito está activado porque un protocolo tenía datos para enviar.

Rmt Disc

Desconectado remotamente. El circuito está desactivado o disponible porque el destino remoto ha desconectado la llamada.

Opr Req

Petición del operador. El circuito está disponible porque un mandato de supervisión ha desconectado la última llamada.

Inbound

El circuito está activado porque el circuito ha respondido a una llamada de entrada.

Restoral

El circuito está activado debido a una operación de Restauración de WAN.

Self Test

El circuito estaba configurado como estático (idle time=0) y se ha conectado satisfactoriamente una vez se ha habilitado.

Duration

Período de tiempo que el circuito ha estado en el estado actual.

Dial-dump

Utilice el mandato **dial-dump** para visualizar las características de funcionamiento del circuito de marcación especificado.

Mandatos de supervisión RDSI

Sintaxis:

dial-dump *circuitname*

L2_Counters

Utilice el mandato **L2_counters** para listar los estados de L2/L1 junto con algunos contadores L2.

Sintaxis:

L2_counters

L3_Counters

Utilice el mandato **L3_Counters** para listar los contadores de configuraciones enviadas/recibidas/aceptadas.**Sintaxis:**

L3_counters

TEI

Utilice el mandato **TEI** para listar el estado de los TEI. Sólo para BRI.

Sintaxis:

parameters

Ejemplo:

parameters

ISDN Port parameters:

Local Address Name: v1233
Local Network Address: 20
Local Network Subaddress:
Frame Size: 2048
TEI 0: Automatic
TEI 1: Automatic

Switch Variant: AT&T 5ESS (United States)
Multipoint Selection: Multipoint
Directory Number 0: 20
Outbound call address Timeout: 180 Retries: 0

Parameters

Utilice el mandato **parameters** para visualizar la configuración RDSI actual.

Sintaxis:

parameters

Ejemplo:

parameters

ISDN Port parameters:

Local Address Name: v1233
Local Network Address: 20
Local Network Subaddress:
Frame Size: 2048
TEI 0: Automatic
TEI 1: Automatic

Switch Variant: AT&T 5ESS (United States)
Multipoint Selection: Multipoint
Directory Number 0: 20
Outbound call address Timeout: 180 Retries: 0

Statistics

Utilice el mandato **statistics** para visualizar las estadísticas actuales para esta interfaz RDSI.

Sintaxis:

statistics

Ejemplo para PRI con E1:

```

statistics
Link: Active ISDN Firmware: 1.0 Handler State: Running

Transmit D Channel Receive D Channel

Packets 68422 Packets 68419
Bytes 411656 Bytes 413592
Overflow 23 Overflow 3
Underrun 0 Too Long 6
Abort 4
CRC error 8
Misaligned 3

Transmit B Channels Receive B Channels

Packets 1499094 Packets 1499228
Bytes 59955660 Bytes 59951780
Overflow 0 Overflow 90
Underrun 0 Too Long 171
Abort 139
CRC error 232
Misaligned 72

E1 Status Register E1 Error Count Registers

Receive AIS : Off CRC6 Errors: 4
Receive RAI : Off LCV Errors: 38
Receive Carrier Loss: Off FEB Errors: 11
Receive Loss of Sync: Off FAS Errors: 24

```

Ejemplo para PRI con T1 que utiliza I.431:

```

statistics
Transmit Receive

Packets 0 Packets 0
Bytes 0 Bytes 0
Overflow 68480 Overflow 0
Underrun 0 Too Long 0
Abort 0
CRC error 0
Misaligned 0

T1 Status Register T1 Error Count Registers

Receive AIS : Off LCV Errors: 0
Receive RAI : Off CRC6 Errors: 0
Receive Carrier Loss: Off Sync Errors: 47937328
Receive Loss of Sync: On

T1 PRM Events Local Remote

CRC Error 0 0
Controlled Slip 0 0
Line Code Violation 0 0
Frame Sync Bit Error 0 0
Severely Errored Frame 0 0
Payload Loopback Active 0 0
PRMs Processed (1/sec) 0 0

```

RDSI y los mandatos GWCON

Aunque RDSI tenga su propio proceso de supervisión, el direccionador también visualiza información de configuración y estadísticas completas para dispositivos y circuitos cuando se utilizan los mandatos **interface**, **statistics**, y **error** en el entorno GWCON. También puede utilizar el mandato **test** de GWCPM para probar los DCE y los circuitos.

RDSI y los mandatos GWCON

Nota: La emisión del mandato **test** para la interfaz RDSI hace que se desactiven y vuelva a marcar las llamadas actuales.

Interfaz — Estadísticas para interfaces RDSI y circuitos de marcación

Utilice el mandato **interface** en el indicador GWCON (+) para visualizar las estadísticas para las interfaces RDSI y los circuitos de marcación.

Para visualizar las estadísticas para un circuito de marcación, entre el mandato **interface** seguido del número de interfaz del circuito de marcación. Para interfaces RDSI, la información se visualiza en base a un canal D y B. (Se trata de la misma información que visualiza el mandato **statistics** de Talk 5 de RDSI.)

Ejemplo:

interface 2

```
Nt Nt' Interface Slot-Port Self-Test Self-Test Maintenance
2 2 ISDN/0 Slot: 8 Port: 1 Passed Failed Failed
1 0 0
```

```
ISDN Base Net MAC/data-link on ISDN Primary Rate interface
Link: Active ISDN Firmware: 1.0 Handler State: Running
```

```
Transmit D Channel Receive D Channel
Packets 36 Packets 36
Bytes 214 Bytes 214
Overflow 0 Overflow 0
Underrun 0 Too Long 0
Abort 0
CRC error 0
Misaligned 0
```

```
Transmit B Channels Receive B Channels
Packets 0 Packets 0
Bytes 0 Bytes 0
Overflow 0 Overflow 0
Underrun 0 Too Long 0
Abort 0
CRC error 0
Misaligned 0
```

T1 Status Register T1 Error Count Registers

```
Receive AIS : Off LCV Errors: 0
Receive RAI : Off CRC6 Errors: 0
Receive Carrier Loss: Off Sync Errors: 0
Receive Loss of Sync: Off
```

```
T1 PRM Events Local Remote
CRC Error 0 0
Controlled Slip 0 0
Line Code Violation 0 0
Frame Sync Bit Error 0 0
Severely Errored Frame 0 0
Payload Looback Active 0 0
PRMs Processed (1/sec) 365 367
```

Para visualizar las estadísticas siguientes para un circuito de marcación, utilice el mandato **interface** seguido del número de interfaz del circuito de marcación.

Ejemplo:

interface 3

```
Nt Nt' Interface Self-Test Self-Test Maintenance
3 2 PPP/1 Passed Failed Failed
1 0 0
```

```
Point to Point MAC/data-link on ISDN Primary Rate interface
```

La lista siguiente describe la salida para RDSI y circuitos de marcación.

Nt El número de interfaz de la línea serie o el número de interfaz del circuito de marcación.

Nt' Si *Nt* es un circuito de marcación, se trata del número de la interfaz RDSI con la que se correlaciona el circuito de marcación.

Interface

El tipo de interfaz y su número de instancia.

Slot La ranura que contiene el adaptador RDSI.

Port El número de puerto del adaptador RDSI.

Self-Test Passed

Número de autopruebas que han sido satisfactorias.

Self-Test Failed

Número de autopruebas que han fallado.

Maintenance: Failed

Número de anomalías de mantenimiento.

Configuración—Información sobre el hardware y el software del direccionador

Entre el mandato **configuration** en el indicador GWCON (+) para visualizar información acerca del hardware y software del direccionador. Incluye una sección que visualiza las interfaces configuradas en el direccionador junto con el estado de la interfaz.

Si un circuito de marcación está configurado para la marcación a petición, el estado del circuito de marcación siempre se visualiza como activado esté o no conectado. En este caso activado significa que el circuito de marcación está conectado o disponible.

Si un circuito de marcación está configurado como un circuito estático, el estado indica sólo activado si el circuito de marcación está conectado. (Consulte la sección "Configuration" en la página 120 para ver una salida de ejemplo del mandato **configuration**.)

Soporte para la reconfiguración dinámica de RDSI

Esta sección describe la reconfiguración dinámica (DR) en la medida en que afecta a los mandatos Talk 6 y Talk 5.

Delete Interface de CONFIG (Talk 6)

La interfaz de bucle de retorno RDSI soporta el mandato **delete interface** de CONFIG (Talk 6) sin ninguna restricción.

Activate Interface de GWCON (Talk 5)

RDSI soporta el mandato **activate interface** de GWCON (Talk 5) sin ninguna restricción.

Reset Interface de GWCON (Talk 5)

RDSI no soporta el mandato **reset interface** de GWCON (Talk 5).

RDSI y los mandatos GWCON

Capítulo 54. Configuración y supervisión de circuitos de marcación

Este capítulo describe cómo configurar los circuitos de marcación en una interfaz de circuito de marcación correlacionada con una interfaz V.25bis o RDSI. Contiene las secciones siguientes:

- “Mandatos de configuración de circuitos de marcación”
- “Mandatos de supervisión de circuitos de marcación” en la página 804
- “Soporte para la reconfiguración dinámica de circuitos de marcación” en la página 804

Notas:

1. Las interfaces de circuitos de marcación PPP pueden utilizar una red RDSI o V.25bis como interfaz de red base.
2. Las interfaces de circuitos de marcación FR pueden utilizar RDSI o una red V.25bis como interfaz de red base.
3. Las interfaces de circuito de llamada de entrada SDLC conmutadas utilizan una red V.25bis como la interfaz de red base.
4. Se pueden utilizar los circuitos X.25 a través de canales D RDSI para BRI.

Para obtener información de cómo configurar los circuitos de marcación para utilizarlos con:

- Interfaces RDSI, consulte la sección “Capítulo 52. Utilización de la interfaz RDSI” en la página 769.
- Interfaces V.25bis, consulte la sección “Capítulo 50. Utilización de la interfaz de red V.25bis” en la página 751.

Mandatos de configuración de circuitos de marcación

La Tabla 103 describe los mandatos de configuración de circuitos de marcación. Entre los mandatos de configuración del circuito de marcación en el indicador `Circuit Config>`. Debe reiniciar el direccionador para que los cambios en la configuración surtan efecto.

Para acceder al indicador `Circuit Config>`, entre el mandato **network** seguido del número de interfaz del “circuito de marcación”. (El número del circuito de marcación se ha asignado cuando ha entrado el mandato **add device dial-circuit**.) Puede entrar el mandato **list devices** en el indicador `Config>` para visualizar una lista de los circuitos de marcación que ha añadido.

Tabla 103. Resumen de los mandatos de configuración de circuitos de marcación

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página 10.
Delete	Suprime los valores de llamada de entrada de la configuración del circuito de marcación.
Encapsulator	Le permite cambiar la configuración del protocolo de enlace de datos.
List	Visualiza los parámetros de configuración del circuito de marcación.

Configuración de circuitos de marcación

Tabla 103. Resumen de los mandatos de configuración de circuitos de marcación (continuación)

Mandato	Función
Set	Configura el circuito de marcación para llamadas de entrada y de salida, correlaciona el circuito de marcación con una interfaz de línea serie y establece las direcciones, el tiempo de espera excedido de desocupado, la prioridad, la dirección de lid_out, el destino de entrada y el retardo de autopruueba.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página 11.

Delete

Utilice el mandato **delete** para eliminar los valores de llamada de entrada de la configuración del circuito de marcación.

Sintaxis:

delete *inbound destino*

inbound destino

Elimina el destino INBOUND y los valores ANY_INBOUND de la configuración del circuito de marcación. Esto hace que el circuito de marcación sólo acepte llamadas de llamadores que tengan un número de teléfono que coincida con el parámetro *destino*.

Encapsulator

Utilice el mandato encapsulator para entrar en el proceso de configuración para el protocolo de capa de enlace (por ejemplo, PPP, Frame Relay, X.25, SDLC) que se ejecuta en la interfaz del circuito de marcación.

Nota: El valor por omisión para una interfaz de circuito de marcación creada mediante el mandato **add device dial-circuit** es PPP. Para cambiar el tipo de capa de enlace en el indicador Config>:

- Para Frame Relay, entre **set data-link frame-relay**.
- Para SDLC, entre **set data-link sdlc**.

Sintaxis:

encapsulator

El ejemplo siguiente muestra que se entra en el proceso de configuración PPP cuando se utiliza el mandato encapsulator para una interfaz de circuito de marcación PPP.

Ejemplo:

```
encapsulator
Point-to-Point user configuration
PPP Config>
```

Asegúrese de lo siguiente cuando configure un circuito de marcación que utiliza una interfaz V.25bis como red base:

- La interfaz V.25bis predefine el cronometraje como externo. El módem (DCE) controla la velocidad de reloj. No puede configurar el cronometraje, la codificación y otros parámetros HDLC como parte de la configuración del circuito de marcación.

Configuración de circuitos de marcación

Tenga en cuenta que no puede configurar parámetros HDLC de la configuración del circuito de marcación cuando configure PPP o Frame Relay para RDSI. Los parámetros de capa física se configuran en la interfaz RDSI.

Para obtener información sobre la configuración del protocolo PPP, consulte la sección “Capítulo 36. Configuración de interfaces de línea serie” en la página 459 o la sección “Capítulo 43. Utilización de interfaces de Point-to-Point Protocol” en la página 621.

Para obtener información sobre la configuración del protocolo Frame Relay, consulte las secciones “Capítulo 41. Utilización de interfaces Frame Relay” en la página 531 o “Capítulo 42. Configuración y supervisión de interfaces Frame Relay” en la página 561.

Para obtener información sobre la configuración o supervisión de las interfaces SDLC, consulte las secciones “Capítulo 48. Utilización de interfaces SDLC” en la página 723 o “Capítulo 49. Configuración y supervisión de interfaces SDLC” en la página 725.

Para obtener información sobre la configuración y supervisión de la interfaz X.25, consulte la sección “Capítulo 38. Configuración y supervisión de la interfaz de red X.25” en la página 469.

Para volver al indicador `Circuit Config>`, utilice el mandato **exit**.

List

Utilice el mandato **list** para visualizar la configuración actual del circuito de marcación.

Para obtener más información acerca de I.430 e I.431, consulte la sección “Variante de conmutador I.431” en la página 781.

Sintaxis:

list

-

Ejemplo:

Nota: Las opciones listadas dependen del tipo de interfaz utilizada. Puede que no se muestren todas las opciones para todos los tipos de interfaz.

```
list
Any inbound          set
Bandwidth:           64
Base net:             1
Callback:             yes
Calls:                inbound
Destination name:    remote-site-sanfrancisco
Idle char:            7E
Idle timer:           = 60 sec
Inbound calls         allowed
Inbound dst name:    local-1
LID out address:     1234
LID used:             enabled
Net #:                2
Outbound calls        allowed
Priority:              8
SelfTest Delay Timer: = 0 ms
Time slot:            1 4 5 8
```

Configuración de circuitos de marcación

Any inbound

Visualiza este valor cuando las llamadas de entrada que no coinciden con ningún otro circuito de marcación se correlacionan con este circuito y se aceptan como llamadas de entrada.

Bandwidth

Visualiza el valor de ancho de banda en kbps.

Base net

Visualiza el nombre de la interfaz de línea serie con el que se correlaciona este circuito de marcación.

Callback

Visualiza el valor de esta opción.

Calls Visualiza el valor de esta opción.

Destination name

Visualiza el nombre de dirección de red que se ha de llamar para circuitos de salida y la dirección de comparación por omisión utilizada por el mecanismo LID para las llamadas de entrada.

Idle char

Visualiza el carácter de desocupado utilizado para circuitos I.43x o canalizados.

Idle timer

Visualiza el valor del temporizador de desocupado en segundos. El rango es de 0 a 65535; 0 indica que se trata de un circuito dedicado (línea alquilada).

Inbound calls allowed

Visualiza este parámetro cuando se configura el circuito para aceptar llamadas de entrada.

Inbound dst name

Visualiza este parámetro si el circuito está configurado para aceptar llamadas de entrada que no coinciden con ninguna otra dirección. Es un nombre de dirección de comparación alternativo utilizado por el mecanismo LID para las llamadas de entrada.

LID out address

Visualiza el nombre del circuito de marcación que conecta los direccionadores.

LID used

Visualiza el valor de esta opción.

Net # Visualiza el número de circuito base.

Outbound calls allowed

Visualiza este parámetro cuando el circuito está configurado para iniciar llamadas de salida.

Priority

Visualiza el valor de este parámetro.

SelfTest Delay Timer

Visualiza el valor del temporizador de retardo de autoprueba en milisegundos. El rango es de 0 a 65535; 0 indica que no hay retardo.

Time slot

Visualiza la lista de ranuras que se han de utilizar para este circuito de marcación.

Set

Utilice el mandato **set** para correlacionar el circuito de marcación con una interfaz (por ejemplo: RDSI o V.25bis), configurar el circuito de marcación para llamadas de entrada y/o de salida y establecer las direcciones de destino, las direcciones de entrada, el tiempo de espera excedido de desocupado y el retardo de autopruueba.

Nota:

Notas:

1. Si ejecuta SDLC, I.430, I.431, Canalizado o X.25 en un circuito de marcación, no podrá utilizar el mandato **set** para cambiar los siguientes parámetros ya que el software utilizará los valores por omisión específicos:
 - Any_inbound - se establece any_inbound
 - Calls - de entrada
 - Destination - dirección por omisión
 - Inbound destination - no hay ninguna dirección de entrada de destino
 - Idle - 0
 - Lid_out_addr - no hay un nombre LID
 - Lid_used - inhabilitado
 - Priority - 8
 - Self_test_delay

Sintaxis:

```

set                               any_inbound
                                   bandwidth...
                                   callback...
                                   calls...
                                   destination...
                                   idle...
                                   idle-char...
                                   inbound destination...
                                   lid_out_addr...
                                   lid_used...
                                   net...
                                   priority...
                                   selftest-delay...
                                   timeslot...

```

any_inbound

Especifica que las llamadas de entrada que no coinciden con ningún otro circuito de marcación se correlacionan con este circuito y se aceptan como llamadas de entrada.

bandwidth *kbps*

Establece el ancho de banda, en kbps, para circuitos I.430 y T1/E1 canalizados.

Valores válidos:

Para I.430: 64 ó 128

Para canalizados: 56 ó 64

Configuración de circuitos de marcación

Valor por omisión: 64

callback [*Sí o No*]

La característica de llamada de retorno utiliza el número de teléfono de los llamadores par verificar la llamada con una tabla de autenticación y, a continuación, desconecta la llamada de entrada. Después, la llamada de retorno efectúa una llamada de salida al mismo llamador. La llamada de retorno debe estar siempre inhabilitada. El valor por omisión es no.

calls [*de salida o de entrada o ambas*]

Restringe el circuito de marcación a sólo iniciar llamadas de salida, sólo aceptar llamadas de entrada o a iniciar y aceptar llamadas. El valor por omisión es ambos.

destination *nombre_dirección*

Este parámetro es necesario para que el circuito de marcación funcione. Especifica la dirección de marcación de red del direccionador remoto con el que se conectará este circuito de marcación. El protocolo LID utiliza este parámetro como dirección de comparación por omisión para llamadas de entrada. Este parámetro debe coincidir con un nombre de dirección que ha asignado utilizando el indicador `Config>` con el mandato **add isdn address** o el mandato **add v25-bis address**.

Ejemplo: `set destination remote-site-sanfrancisco`

idle *núm. de segundos*

Especifica un período de tiempo de espera excedido para el circuito. Si no hay tráfico de protocolo a través del circuito durante este período de tiempo especificado, el circuito de marcación queda en suspenso. El rango es de 0 a 65535 y el valor por omisión es de 60 segundos. Un valor de cero especifica que no hay período de tiempo de espera excedido y que se trata de un circuito dedicado.

Notas:

1. Para las operaciones de Restauración de WAN, debe establecer el tiempo de espera excedido de desocupado en 0.
2. En un circuito I.43x, X.25 o Canalizado, no puede establecer este parámetro.

idle-char

Especifica el carácter de desocupado utilizado para circuitos canalizados.

Nota: No puede configurar este parámetro para circuitos RDSI regulares.

Valores válidos: 7E o FF

Valor por omisión: FF

Ejemplo: `set idle-char 7E`

inbound-destination *nombre_dirección*

Establezca este parámetro si el circuito de marcación está configurado para llamadas de entrada y de salida y si la dirección de marcación local del direccionador es diferente de la dirección de marcación de destino que marca el direccionador remoto. Por ejemplo, los números pueden ser diferentes si uno de los direccionadores pasar a través de un intercambio PVX, internacional o inter-LATA. Este parámetro debe coincidir con un nombre de dirección que haya asignado en el indicador `Config>` con el mandato **add isdn address** o el mandato **add v25-bis address**. El número

Configuración de circuitos de marcación

de destino de entrada se utiliza para emparejar el LID de entrada o CallerID con el circuito de marcación. Si existe una coincidencia, este circuito de marcación recibe la llamada.

Ejemplo: set inbound remote-site-1

lid_out_addr *nombre_dirección*

lid_out_addr es el nombre de un circuito de marcación entre dos direccionadores. Cuando hay más de un circuito configurado entre dos direccionadores (circuitos paralelos), debe haber una manera de saber sin ambigüedad qué circuito de marcación los conecta. Para esta finalidad, se envía un lid_out_addr desde el direccionador a un extremo (el llamador). En el extremo receptor, el otro direccionador configura la misma serie como el nombre de destino de entrada. lid_out_addr debe ser un nombre de dirección que se haya añadido previamente utilizando **ADD RDSI-ADDRESS** en el indicador config>.

lid_used [yes o no]

Suprime el intercambio de id lógicos para circuitos con dispositivos que no soportan id lógicos.

Valores válidos: Yes o No

Valor por omisión: Yes

net *número*

Establece el número de red base de la interfaz en el *número* de la interfaz de línea serie con el que desea correlacionar este circuito.

Ejemplo:

```
Circuit Config> set net
Base net for this circuit [ ]? 2
```

priority

El campo de prioridad permite que un circuito de marcación a petición de salida sustituya a otro cuando no hay ningún canal disponible. Si se efectúa una petición y se están utilizando todos los canales, se comprueba la prioridad del circuito de marcación a petición solicitante con todos los circuitos de marcación a petición activos. Si hay un circuito de marcación a petición de salida con una prioridad inferior, se desconecta y se efectúa una llamada para el circuito de marcación a petición con la prioridad superior. Sólo se considera la prioridad en el extremo de salida de una petición. No se desactivará una llamada de marcación a petición de entrada en favor de una llamada de salida de prioridad superior. Una llamada de marcación a petición de entrada no puede provocar que una llamada de prioridad inferior se desactive.

selftest-delay *núm. de milisegundos*

Utilice este parámetro para retardar el tiempo entre el establecimiento de la llamada y el momento del envío del paquete inicial. El establecimiento de un retardo de autoprueba puede evitar que se eliminen paquetes iniciales. El rango es de 0 a 65535 y el valor por omisión es 150.

Para los circuitos de marcación V.25bis, ajuste este valor si los módems tardan un tiempo en sincronizarse.

Para los circuitos de marcación RDSI, puede ser necesario ajustar este valor para los enlaces de marcación a petición, porque algunos conmutadores RDSI empiezan a entregar los datos antes de señalar el establecimiento completo del circuitos en el extremo de destino.

Delete Interface de CONFIG (Talk 6)

Los Circuitos de marcación soportan el mandato **delete interface** de CONFIG (Talk 6) sin ninguna restricción.

Activate Interface de GWCON (Talk 5)

Los Circuitos de marcación soportan el mandato **activate interface** de GWCON (Talk 5) con la consideración siguiente:

La red base ya debe estar activada. Consulte las restricciones específicas de los enlaces de datos.

Reset Interface de GWCON (Talk 5)

Los Circuitos de marcación soportan el mandato **reset interface** de GWCON (Talk 5) con la consideración siguiente:

No puede restablecer una interfaz de Circuito de marcación si ha cambiado algún parámetro del Circuito de marcación. El restablecimiento está permitido si los únicos parámetros que cambia el mismo están asociados a los enlaces de datos que se ejecutan en la parte superior del circuito. Estos parámetros tienen restricciones asociadas a estos enlaces de datos.

Parte 4. Apéndices

Apéndice A. Consulta para la configuración rápida

Importante

Si está intentando configurar o supervisar el IBM 2216 y no se puede leer el terminal de servicio, consulte la sección "Service Terminal Display Unreadable" en la publicación 2216 Nways Multiaccess Connector Service and Maintenance Manual.

Consejos para la configuración rápida

Antes de empezar el proceso de Configuración rápida, lea estas notas:

1. Conecte un terminal ASCII al puerto de servicio para ejecutar el programa de Configuración rápida. Consulte la publicación *Installation and Initial Configuration Guide*.
2. Se eliminará cualquier configuración existente para un elemento en particular si ese elemento se ha configurado mediante la Configuración rápida.
3. La configuración se realiza a nivel de la *interfaz*, lo que corresponde a un solo *puerto* de un adaptador. Puesto que los distintos tipos de adaptadores tienen números de puertos diferentes, puede tener que configurar hasta ocho puertos para activar todas las interfaces del adaptador (por ejemplo, el adaptador X.21, FC 2291).

Nota: El adaptador ESCON o PCA pueden tener hasta 16 interfaces virtuales configuradas en una interfaz física. Todas las interfaces virtuales están asociadas a un sólo puerto.

4. Si utiliza el mandato **add device**, debe "añadir" todas las interfaces de red deseadas o interfaces virtuales para los adaptadores instalados en el IBM 2216. Esto debe realizarse antes de ejecutar la Configuración rápida. Para añadir una interfaz, consulte la sección "Add" en la página 77.
5. Si utiliza el mandato **network**, debe entrar la información de configuración de la interfaz de red. Consulte la sección "Network" en la página 102.

Selecciones

En los paneles del programa Configuración rápida, la información que aparece entre corchetes, [], es el valor por omisión. Por ejemplo:

Configure Bridging? (Yes, No, Quit): [Yes]

- Para utilizar el valor por omisión Yes, pulse **Intro**.
- Para utilizar un valor que no sea el valor por omisión como, por ejemplo, No o Quit, elija entre los valores entre paréntesis.
- Si no aparece ningún valor entre corchetes, es que no hay valor por omisión y debe escribir un valor.

Salida y Reinicio

- Para reiniciar la sección de configuración rápida actual en cualquier momento, escriba **r**. Por ejemplo, si está en la sección de configuración de interfaces, escriba **r** y pulse **Intro** para volver al principio de esa sección.
- Para salir de la configuración rápida, escriba **q** y pulse **Intro**. Aparecerá el indicador Config>.

- Para reiniciar la configuración rápida desde el indicador Config>, escriba **qc** y pulse **Intro**.

Cuando haya terminado

- Cuando haya completado la configuración, debe reiniciar el dispositivo para que la configuración surta efecto. Se proporciona esta opción al final del programa de Configuración rápida.

Inicio del programa de Configuración rápida

Las secciones siguientes describen configuraciones de ejemplo que utilizan el programa de Configuración rápida (**qconfig**).

Para iniciar el programa de configuración rápida, entre **qc** en el indicador Config>.

El programa visualiza el siguiente panel después del inicio.

```
Router Quick Configuration for the following:
o Bridging
  Spanning Tree Bridge (STB)
  Source Routing Bridge (SRB)
  Source Routing Transparent Bridge (SRT)
o Protocols
  IP (including OSPF, RIP, and SNMP)
  IPX
  DNA (DECnet)

Event Logging will be enabled for all configured subsystems
with logging level 'Standard'

Note: Please be warned that any existing configuration for a particular item
will be removed if that item is configured through Quick Configuration
```

El *Registro cronológico de sucesos* anota la actividad del sistema, los cambios de estado, la transmisión y recepción de datos, los errores de datos e los internos y las peticiones de servicio. El nivel de anotación cronológica se establece en estándar (el valor por omisión). Para obtener información acerca del registro de errores, consulte la publicación *event Logging System Messages Guide*.

Durante la configuración rápida puede:

1. Configurar el puente
2. Configurar protocolos
3. Reiniciar el dispositivo

Configuración de LAN Emulation

Si ha añadido un dispositivo ATM, verá las siguientes solicitudes:

```

*****
LAN Emulation Configuration
*****

Type 'Yes' to Configure LAN Emulation
Type 'No' to skip LAN Emulation Configuration
Type 'Quit' to exit Quick Config

Configure LAN Emulation? (Yes, No, Quit): [Yes]

```

Puede configurar clientes de LAN Emulation de Red en Anillo o Ethernet a partir de esta pregunta.

Configuración de la función de puente

```

*****
Bridging Configuration
*****

Type 'Yes' to Configure Bridging
Type 'No' to skip Bridging Configuration
Type 'Quit' to exit Quick Config

Configure Bridging? (Yes, No, Quit): [Yes]

```

1. En respuesta a Configure Bridging, lleve a cabo alguna de las acciones siguientes:
 - Entre **y** para visualizar las solicitudes de la configuración de la función de puente. Las solicitudes que aparecen dependen de la configuración de la red.
 - Entre **n** para saltarse la configuración de la función de puente y continuar con la configuración rápida.
 - Entre **q** para salir de la configuración rápida. Esto visualiza el indicador Config>. Para volver a entrar en la configuración rápida, entre **qc** después de esta solicitud.
2. Si elige configurar la función de puente, se habilitará la Función puente de árbol de expansión (STB) en todas las interfaces LAN. Verá los paneles siguientes:

```

Type 'r' any time at this level to restart Bridging Configuration

STB will be enabled on all LAN interfaces

```

Entre **y** para configurar la función de puente SRT. De lo contrario, entre **n**. Para cada interfaz de Red en Anillo de la configuración, se le solicitará que habilite el Direccionamiento de origen en la interfaz.

```

Configure SRT Bridging? (Yes, No): [Yes]
You are now configuring the Source Routing part of SRT Bridging
Bridge Number (hex) of this Router (1-F): [A]

```

3. Entre un número de puente, que es un valor hexadecimal de 1 a F exclusivo entre dos segmentos paralelos.

```

Interface 0 (Port 1) is of type Token Ring
Configure Source Routing on this interface (Yes, No): [Yes]

```

4. Entre **y** para configurar el direccionamiento de origen en la interfaz. La consola visualiza las dos líneas siguientes.

```
Configuring Interface 0 (Port 1)
Segment Number (hex) of this Interface (1-FFF): [A1]
```

Nota: El número de puerto se incrementa en uno porque la función de puente de direccionamiento de origen no permite el número de puerto cero.

Se asigna un valor hexadecimal exclusivo de 1 a FFF a cada interfaz. Las interfaces de cada anillo (segmento) tienen el mismo número de segmento, pero el número de segmento es exclusivo para cada anillo.

Aparecen estas solicitudes para cada interfaz de Red en Anillo.

```
Interface 1 (Port 2) is of type Token Ring
Configure Source Routing on this interface? (Yes, No): [Yes]
Configuring Interface 1 (Port 2)
Segment Number (hex) of this Interface (1-FFF): [A2]
```

Si hay más de dos interfaces configuradas para el direccionamiento de origen, entre un valor hexadecimal exclusivo de 1 a FFF para el segmento virtual interno.

```
Virtual Segment Number (hex) of this Router (1-FFF): [A4]
```

5. Se visualiza un panel similar al siguiente:

```
This is all configured bridging information:

  Interfaces configured for STB:

  Interface #   Port #   Interface Type
  -----
           0         1       Token Ring
           1         2       Token Ring

The Source Routing part of SRT Bridging has been enabled

Bridge Number of this Router: A

Interfaces configured for Source Routing:

  Interface #   Port#   Segment #   Interface Type
  -----
           0         1         A1       Token Ring
           1         2         A2       Token Ring

Virtual Segment Number of this Router: A4

Save this Configuration? (Yes, No): [Yes]
```

6. Entre **y** para guardar la configuración de la función de puente y continuar con la configuración rápida. Entre **n** para volver a visualizar las solicitudes de configuración de la función de puente.

Si entra **y**, aparece el mensaje siguiente:

```
Bridging configuration saved
```

Configuración de protocolos

Después de guardar la configuración de la función de puente, verá el panel siguiente:

```

*****
Protocol Configuration
*****

Type 'Yes' to Configure Protocols
Type 'No' to skip Protocol Configuration
Type 'Quit' to exit Quick Config

Configure Protocols? (Yes, No, Quit): [Yes]

```

Lleve a cabo una de las acciones siguientes:

- Entre **y** para configurar los protocolos.
- Entre **n** para saltarse la configuración de protocolos y continuar con la configuración rápida.
- Entre **q** para salir de la configuración rápida.

Primero configurará IP, después IPX y por último DECnet.

Configuración de IP

Cuando responde **y** al panel Configure Protocol, la configuración rápida visualiza los mensajes siguientes:

```

Type 'r' any time at this level to restart Protocol configuration

Configure IP? (Yes, No): [Yes]

```

1. Lleve a cabo una de las acciones siguientes:

- Entre **y** para configurar IP.
- Entre **n** para saltarse la configuración IP y continuar con la configuración rápida.

Aparecen las líneas siguientes para cada interfaz.

```

Configuring Per-Interface IP Information

Type 'Yes' to Configure IP on this interface
Type 'No' to skip to the next interface
Type '?' to list interfaces
Type an interface # to skip to that interface
Type 'Quit' to exit Per-Interface IP Configuration

Configure IP on Interface 0 (Token Ring)?
(Yes, No, #, ?, Quit) [Yes]
IP Address: [] 128.185.141.1
Address Mask: [255.255.0.0]

```

2. Entre la dirección IP en notación decimal, por ejemplo, 128.185.142.20. La consola visualiza uno de los siguientes mensajes de error si entra una dirección IP no válida:

```
Bad address, please try again.
```

```
This address has already been assigned. Enter a different address
```

La máscara de red es un valor decimal que refleja la red o subred IP a la que esta interfaz está conectada.

Para obtener más información acerca del direccionamiento IP o de las máscaras de dirección, consulte la publicación *Consulta de configuración y supervisión de protocolos* o consulte al administrador de la red.

```
Per-Interface IP Configuration complete
```

```
Configuring IP Routing Information  
Enable Dynamic Routing (Yes, No): [Yes]
```

- Entre **y** si desea que los protocolos de direccionamiento (RIP o OSPF) creen las tablas de direccionamiento. Entre **n** para añadir manualmente los destinos de dirección IP a las tablas de direccionamiento (rutas estáticas).

```
Enable OSPF? (Yes, No): [Yes]
```

- Entre **y** para habilitar el protocolo de direccionamiento OSPF como el protocolo de direccionamiento IP dinámico primario. RIP sólo se habilitará para enviar anuncios, no para recibirlos. Entre **n** si no desea utilizar OSPF. RIP se habilitará para enviar y recibir anuncios.

```
OSPF Enabled with Max routes = 1000 and Max routers = 50
```

Max routes es el número máximo de rutas externas de sistemas autónomos (AS) importadas al dominio de direccionamiento OSPF. Max routers es el número máximo de direccionadores OSPF del dominio de direccionamiento.

```
Routing Configuration Complete
```

```
SNMP will be configured with the following parameters:
```

```
Community: public  
Access: READONLY
```

```
If you plan to use the graphical configuration tool  
to download a configuration, it requires the definition  
of a community name with read_write_trap access.
```

```
Define community with read_write_trap access ? (Yes, No): [Yes]
```

```
This is the information you have entered:
```

Interface #	IP Address	Address Mask
0	128.185.141.1	255.255.255.0
1	128.185.142.1	255.255.255.0
2	128.185.143.1	255.255.255.0

```
OSPF is configured, and RIP is configured only for 'sending'
```

```
SNMP has been configured with the following parameters:
```

```
Community: public  
Access: read_trap  
  
Community: dana  
Access: read_write_trap
```

```
Save this configuration? (Yes, No): [Yes]
```

- Entre **y** para guardar la configuración IP y continuar con la configuración rápida. Entre **n** para volver a visualizar las solicitudes de configuración de protocolo.

Configuración de IPX

Después de guardar la configuración IP, verá los mensajes siguientes:

Configure IPX? (Yes, No): [Yes]

1. Entre **y** para configurar IPX. Entre **n** para saltarse la configuración de IPX y continuar con la configuración rápida.

Verá mensajes similares al siguiente:

```
Type 'r' any time at this level to restart IPX Configuration
IPX Configuration is already present
Configure IPX anyway? (Yes, No): [No] yes
```

2. Entre **y** para sustituir la configuración existente. Entre **n** para conservar la configuración actual y continuar.

Configuring Per-Interface IPX Information

```
Type 'Yes' to Configure IPX on this interface
Type 'No' to skip to the next interface
Type an interface # to skip to that interface
Type '?' to list interfaces
Type 'Quit' to exit Per-Interface IPX Configuration
```

```
Configure IPX on Interface 0 (Token Ring)?
(Yes, No, #, ?, Quit) [Yes]
```

3. Los siguientes mensajes y las respuestas dependen de si está configurando Red en anillo, FDDI o Ethernet.

Configuración de la interfaz 0 (Red en anillo):

- a. Se visualiza la siguiente solicitud:

```
Token Ring encapsulation (frame) type? (TOKEN-RING MSB, TOKEN-RING LSB,
TOKEN-RING_SNAP MSB, TOKEN-RING_SNAP LSB): [TOKEN-RING MSB]
```

- b. Entre el tipo de encapsulación utilizado por el protocolo IPX en las estaciones finales de Red en Anillo.

MSB de Red en Anillo: El tipo más normal de encapsulación y el valor por omisión. El IBM 2216 crea paquetes de salida con una cabecera 802.2 de 3 bytes, (0xE0, 0xE0, 0x03). Envía las direcciones de origen y de destino en formato MSB (bit más significativo) o no canónico que es el formato de dirección nativa para la Red en Anillo.

LSB de Red en Anillo Igual que MSB de Red en Anillo excepto en que el IBM 2216 envía las direcciones en formato LSB (bit menos significativo) o canónico.

MSB SNAP de Red en Anillo El IBM 2216 crea paquetes de salida con una cabecera 802.2/SNAP de 8 bytes (0xAA, 0xAA, 0x03, 0x00, 0x00, 0x00, 0x81, 0x37). Envía las direcciones de origen y de destino en formato de bit más significativo (MSB) o no canónico.

LSB SNAP de Red en anillo Igual que MSB SNAP de Red en Anillo excepto en que el IBM 2216 envía las direcciones en formato LSB o canónico.

Configuración de IPX para Ethernet:

- a. Se visualizan las solicitudes siguientes:

```
Ethernet encapsulation type? (ETHERNET_8022, ETHERNET_8023, ETHERNET_ii, ETHERNET_SNAP): [ETHERNET_8023]
```

- b. Entre el tipo de encapsulación utilizado por el protocolo IPX en las estaciones finales Ethernet.

Ethernet_8022	El paquete incluye una cabecera 802.2
Ethernet_8023	Utiliza un formato de paquete IEEE 802.3 sin la cabecera 802.2. Es el valor por omisión y también es el valor por omisión para las versiones de NetWare anteriores a 4.0. Ethernet 802.3 no se ajusta a los estándares IEEE 802 porque no incluye una cabecera 802.2. Puede causar problemas con otros nodos de la red.
Ethernet_II	Utiliza Ethernet tipo 8137 como formato de paquete. Este formato es necesario si está utilizando NetWare VMS en la Ethernet. Es el valor por omisión para NetWare Versiones 4.0 y posteriores.
Ethernet_SNAP	Utiliza el formato 802.2 con una cabecera SNAP. Este tipo de encapsulación está pensado para ser compatible con la encapsulación SNAP de red en anillo. Sin embargo, viola los estándares IEEE y no puede interoperar a través de puentes que lo conforman.

Configuración de IPX para FDDI:

- a. Se visualizan las solicitudes siguientes:

```
FDDI encapsulation (frame) type? (FDDI, FDDI_SNAP): [FDDI_SNAP]
```

- b. Entre el tipo de encapsulación utilizado por el Protocolo IPX para las estaciones finales FDDI.

fddi	Establece el tipo de encapsulación en FDDI IEEE 802.2.
fddi_snap	Establece el tipo de encapsulación en FDDI SNAP.

```
Network Number (hex) (1-FFFFFFFD):[1] 1
```

4. Asigne un número de red IPX a la red asociada conectada directamente. Cada interfaz IPX debe tener un número de red exclusivo.

```
Configure IPX on Interface 1 (WAN PPP)
(Yes, No, #, ?, Quit) [Yes]
Network Number (hex) (1-FFFFFFFD): [1] 2

Enable IPXWAN? (Yes, No): [No] yes

Configure IPS on Interface 2 (WAN PPP)
(Yes, No, #, ?, Quit) [Yes]
Network Number (hex) (1-FFFFFFFD):[1] 3

Enable IPXWAN? (Yes, No): [No] yes

Host Number for Serial Lines: (000000000000) 1

Configure IPXWAN NodeID? (Yes, No): [Yes]
NodeID (hex) (1 - FFFFFFFD): [1] 4
```

Si está habilitado, el protocolo IPXWAN negocia los parámetros de direccionamiento que se han de utilizar en la interfaz serie PPP antes de que empiece el reenvío de paquetes IPX. IPXWAN no es necesario para reenviar

paquetes IPX en interfaces serie PPP. El ID de nodo IPXWAN es un número de red IPX exclusivo que identifica el direccionador y es necesario si IPXWAN está habilitado en cualquiera de las interfaces de red.

5. El número de sistema principal es un valor exclusivo de 12 dígitos hexadecimales asignado a un direccionador IPX. Es necesario porque las líneas serie no tienen direcciones de nodo de hardware a partir del cual se pueda crear un número de sistema principal.

This is the information you have entered:

Per-Interface Configuration Information

Cir	Ifc	IPX Net(hex)	Encapsulation	IPXWAN
1	1	10	ETHERNET_8023	Not Configured
2	3	300		Not Configured
3	5	400		Not Configured
4	6	600		Enabled

Host Number for Serial Lines: 0002210A0000
IPXWAN Node ID = 2210A
IPX Router Name = ipxwan_router-2210A

Save this configuration? (Yes, No): [Yes]

6. Entre **y** para guardar la configuración IPX y continuar con la configuración rápida. Entre **n** para volver a visualizar las solicitudes de configuración IPX. Si entra **y**, aparece el mensaje siguiente:

IPX configuration saved

Configuración DECnet (DNA)

Después de guardar la configuración IPX, verá los mensajes siguientes.

IPX Configuration saved

Configure DNA? (Yes, No): [Yes]

1. Entre **y** para configurar DNA. Entre **n** para saltarse la configuración DNA y continuar con la configuración rápida.

Type 'r' any time at this level to restart DNA Configuration

Configuring Global DNA information

Highest Node Number (decimal) (1-1023): [32]
Router Level (Level1, Level2, DEC Level1, DEC Level2):
[Level2]
Highest Area (decimal) (1-63): [63]
Node Address (area.node): (63.32)

Los campos de configuración anteriores se configuran con las consideraciones siguientes:

Highest Node Number

Es la dirección de nodo superior del área del direccionador. Si se establece excesivamente alto afectará a la eficacia de los direccionadores y necesitará un almacenamiento excesivo.

Router Level

Identifica si el direccionador es de Nivel 1 o de Nivel 2. Un direccionador de Nivel 1 hace un seguimiento de todos los nodos de

este área y no toma en consideración los nodos fuera de su área. Un direccionador de Nivel 2 direcciona el tráfico entre las áreas.

Normalmente, debe seleccionar Level1 o Level2 con la siguiente excepción: seleccione DEC Level1 o DEC Level2 sólo cuando este direccionador debe comunicarse a través de redes X.25 con direccionadores que se ajustan al estándar DEC X.25.

Highest Area

Este número debe ser cómo mínimo tan alto como el número de área más alto de toda la red.

Node Address

Es el ID de nodo de este direccionador y debe ser exclusivo en la red.

Cuando pulse Intro, se visualiza lo siguiente:

```
Configuring Per-Interface DNA Information
Configuring Max Routers on each interface

Configuring Interface 0 (Ethernet)
Configure DNA on this interface? (Yes, No) [YES]
Max Routers (decimal) (1-33): [16]

Configuring Interface 1 (WAN PPP)
Configure DNA on this interface? (Yes, No) [Yes]

Configuring Interface 2 (Token Ring)
Configure DNA on this interface? (Yes, No) [Yes]
Max Routers (decimal) (1-33): [16]
```

2. Entre **y** para cada interfaz que se conectará a la red DECnet. Para las LAN, Max Routers especifica cuántos direccionadores más pueden haber en este circuito. Como requisito para la eficacia y memoria del direccionador establezca este argumento en unos cuantos más que el número total de direccionadores adyacentes de este circuito.

Se visualiza el siguiente panel:

```
This is the information you have entered:

Global Configuration Information

Highest Node Number:      32
Router Level:             Level2
Highest Area:             63
Node Address:             63.32

Pre-Interface Configuration Information
Interface Number          Max Routers

0                          16
1                          1
2                          16

Save this configuration? (Yes, No): [Yes]
```

3. Entre **y** para guardar la configuración DECnet y continuar con la configuración rápida. Entre **n** para volver a visualizar las solicitudes de configuración DECnet. Si entra **y**, aparece el mensaje siguiente:

DNA Configuration Saved

Volver a cargar el dispositivo

Después de la configuración de los protocolos, recibirá el mensaje siguiente:

```
Quick Config Done
Do you want to write this configuration? (Yes, No): [Yes]
```

Entre **y** para guardar los cambios y visualizar la información siguiente:

```
Default config file written successfully.

Configuration was written.
The system must be restarted for this configuration to take effect.
```

Entre **reload** en el indicador OPCON (*) para volver a cargar el dispositivo con la nueva configuración. Para cambiar o ver la configuración actual, entre **qc**.

Apéndice B. Personalidades nacionales X.25

Este apéndice lista los valores por omisión para GTE-Telenet y DDN.

GTE-Telenet

Los parámetros siguientes son los valores por omisión para GTE-Telenet:

- Callreq: 20
- Clearreq:
 - Retries: 1
 - Timer: 18
- Disconnect: Passive
- DP-timer: 500 milisegundos
- Frame window size: 7
- Network Type: CCITT
- N2 timeouts: 20
- Packet:
 - Default size: 128
 - Maximum size: 256
 - Window size: 2
- Reset
 - Retries: 1
 - Timer: 18
- Restart
 - Retries: 1
 - Timer: 18
- Standard: 1984
- T1-timer: 4
- T2-timer: 2

DDN

Los parámetros siguientes son los valores por omisión para DDN:

- Callreq: 20
- Clearreq:
 - Retries: 1
 - Timer: 18
- Disconnect: Passive
- DP-timer: 500 milisegundos
- Frame window size: 7
- Network Type: CCITT
- N2 timeouts: 20
- Packet:
 - Default size: 128
 - Maximum size: 256
 - Window size: 2
- Reset
 - Retries: 1
 - Timer: 18

- Restart
 - Retries: 1
 - Timer: 18
- Standard: 1984
- T1-timer: 4
- T2-timer: 2

Apéndice C. Creación de un archivo de carga del direccionador a partir de múltiples discos

Si la carga de software llega en varios discos, utilice el procedimiento de las secciones siguientes para combinar las cargas en un archivo de carga que el direccionador pueda utilizar en el momento de arranque.

El primer disco contiene los cuatro archivos siguientes que necesita si desea fragmentar una carga existente para el transporte en múltiples disquetes.

cutup.c

(Archivo fuente UNIX C que puede compilarse utilizando un compilador C estándar)

cutup.exe

(DOS)

Utilice los archivos siguientes para volver a ensamblar los fragmentos de carga en un servidor DOS o UNIX.

kopy.bat

(DOS)

kopy (Script de shell UNIX)

Ensamblaje de un archivo de carga bajo DOS

Para ensamblar una carga a partir de dos disquetes, utilice el archivo de proceso por lotes DOS proporcionado en el disquete 1 (KOPY.BAT) utilizando la sintaxis siguiente:

```
kopy <unidad_instalación><directorio_destino>
```

Antes de ensamblar la carga, asegúrese de haber creado un directorio de destino y de que ha insertado el primer disquete en la unidad especificada en el parámetro `unidad_disquete_instalación`. El ejemplo siguiente ilustra este procedimiento.

```
B:\>kopy b: c:\source\cutup\tmp
B:\>copy c:\gw0/B c:\source\cutup\tmp\gw.tmp
1 file(s) copied
.
Please mount the second diskette
Press any key to continue . . .
Copying the second load file fragment
B:\>
B:\>copy c:\source\cutup\tmp\gw.tmp/B + b:\gw1
c:\source\cutup\tmp\gw.tmp c:\SOURCE\CUTUP\TMP\GW.TMP
B:\GW1
1 file(s) copied
B:\>rename c:\source\cutup\tmp\gw.tmp gw.ldc
Load file reassembly was successful
B:>
```

Ensamblaje de un archivo de carga bajo UNIX

Para ensamblar una carga a partir de dos disquetes UNIX, utilice el script de shell Bourne de UNIX (`kopy`) proporcionado en el disquete 1, utilizando la sintaxis siguiente:

```
kopy<unidad_instalación><directorio_disquete><directorio_destino>
```

Antes de ensamblar la carga, asegúrese de que ha creado los directorios de montaje y de destino y de que ha insertado el primer disquete en la unidad especificada por el parámetro `unidad_disquete_instalación`. El ejemplo siguiente ilustra este procedimiento.

```
kopy /dev/fd0 /kew /pcfs

Please insert the first diskette

Copying the first load file fragment

Please mount the second diskette

Copying the second load file fragment

Load file reassembly was successful

# ls /kew

gw0 gw1 gw.ldc
```

Si no puede utilizar el script de shell Bourne de UNIX, puede ensamblar la carga manualmente utilizando el procedimiento siguiente:

1. Copie los fragmentos de carga de los dos disquetes (gw0 y gw1) en un directorio del sistema de archivos UNIX.
2. Escriba el mandato UNIX siguiente:

```
cat gw0 gw1 > gw.ldc
```

El archivo resultante (gw.ldc) es la carga del direccionador ensamblada.

Desensamblaje de un archivo de carga bajo DOS

Para desensamblar una carga bajo DOS, utilice el archivo CUTUP.EXE de la manera siguiente:

```
cutup<extensión_archivo><nombre_archivo><longitud_corte>
```

La extensión_archivo se adjunta al principio parte frontal de cada porción que es necesario cortar. El nombre_archivo es el nombre de archivo DOS del archivo que se va a desensamblar. La longitud_corte es la longitud de cada fragmento que CUTUP.EXE crea al desensamblar el archivo. El ejemplo siguiente ilustra este procedimiento.

```
C: \source\cutup>dir
Volume in drive C has no label
Volume Serial Number is XXXXXXXX
Directory of C: \SOURCE\CUTUP
.0730934:46p
..0730934:46p
GW      LDC 10225660728931:22p
CUTUP  EXE 105410902939:38a
2 file(s) 1033107 bytes
14811136 bytes free
C: \source\cutup>cutup gw.ldc gw 1000000
.....
.....
c: \SOURCE\CUTUP>dir
Volume in drive C has no label
Volume Serial Number is XXXXXXXX
Directory of C: \SOURCE\CUTUP
.0730934:46p
..0730934:46p
GW      0 10000000801931:22p
GW      LDC 10225660728931:22p
CUTUP  EXE 105410902939:38a
GW      1 225660801931:22p
4 file(s) 2055673 bytes
14811136 bytes free
```

Desensamblaje de un archivo de carga bajo UNIX

Para desensamblar una carga bajo UNIX, utilice cutup.c. Empiece por compilar el programa utilizando el compilador UNIX para crear un archivo ejecutable de corte. Después utilice la sintaxis siguiente:

```
cutup<extensión_archivo><nombre_archivo><longitud_corte>
```

La extensión_archivo se adjunta al principio parte frontal de cada porción que es necesario cortar. El nombre_archivo es el nombre de archivo DOS del archivo que se va a desensamblar. La longitud_corte es la longitud de CUTUP.EXE que se utiliza para desensamblar el archivo. El ejemplo siguiente ilustra este procedimiento.

```
# ls -la
total 658
drwxrwxr-x  2 root   512 Aug 114:41 .
drwxrwxr-x 26 root  1024 Aug 114:41 ..
drwxrwxr-x  2 root 24576 Aug 114:41 cutup
drwxrwxr-r  2 root1022566 Aug 114:41 gw.ldc

# cutup gw.ldc gw 100000

# ls -la
total 658
drwxrwxr-x  2 root   512 Aug 114:41 .
drwxrwxr-x 26 root  1024 Aug 114:41 ..
drwxrwxr-x  2 root 24576 Aug 114:41 cutup
drwxrwxr-r  2 root1022566 Aug 114:41 gw.ldc
drwxrwxr-r  2 root1000000 Aug 114:41 gw0
drwxrwxr-r  2 root  22566 Aug 114:41 gw1
```

Apéndice D. Atributos remotos AAA

Esta sección identifica los Atributos AAA remotos que los servidores Radius, TACACS y TACACS+ utilizan.

Radius

ID de proveedor IBM: 211

Atributos de autorización

Estándar preparado

TUNNEL_TYPE	64
TUNNEL_MEDIUM_TYPE	65
TUNNEL_CLIEN_TYPE	66
TUNNEL_SERVER_EP	67
TUNNEL_CONN_ID	68
TUNNEL_PASSWORD	69

valores

TUNNEL_TYPE		entero
1	PPTP	
2	L2F	
3	L2TP	
TUNNEL_MEDIUM_TYPE		entero
1	IP	
TUNNEL_SERVER_EP		serie
	dirección ip	

Específico de proveedor IBM

NAS_TUNNEL_PASSWORD	101
INBYTES_AH	110
INBYTES_ESP	111
OUTBYTES_AH	112
OUTBYTES_ESP	113
INPKTS_BAD	114
OUTPKTS_BAD	115
INPKTS_BAD_AH	116
INPKTS_BAD_ESP	117
OUTPKTS_BAD_AH	118
OUTPKTS_BAD_ESP	119
INPKTS_AH	120
AH INPKTS_ESP	121
OUTPKTS_AH	122
AH OUTPKTS_ESP	123

INPKTS_BAD_AH_RPLY	124
INPKTS_BAD_ESP_RPLY	125
INBYTES_WRAP	128
OUTBYTES_WRAP	129
INB_AH_WRAP	130
INB_ESP_WRAP	131
OUB_AH_WRAP	132
OUB_ESP_WRAP	133
POLICY_NAME	135
P1_ID	136
TRANSFORMS	137
REFR_CNT	138
COMPR	139
ESP_ALGO	140
AH_ALGO	141
ESPAUTH_ALGO	142
P1_NAME	143
VC-ACTIVE	177
VC-IDLETIME	179
VC-SUSPENDTIME	180
CALLBACK_FLAGS	210
ENCRYPTION	211
HOSTNAME	213
SUBNETMASK	215
PRIVILEGE	216

Palabras clave

Las palabras clave se utilizan para servidores Radius que permiten la entrada de campos específicos de proveedores <palabraclave>=<valor>.

KWD_VC_ACTIVE	VCN
KWD_VC_IDLETIME	VCI
KWD_VC_SUSPENDTIME	VCS
KWD_CALLBACK_FLAGS	CBF
KWD_ENCRYPTION	ENC
KWD_HOSTNAME	HSN
KWD_SUBNETMASK	SNM
KWD_PRIVILEGE	PRV

Valores

CALLBACK_FLAGS	
REQ	llamada de retorno necesaria
ROAM	llamada de retorno voluntaria

PRIVILEGE:
 ADMIN
 OPER
 MONITOR

Ejemplo de archivo de configuración RADIUS

El siguiente ejemplo es un archivo de configuración RADIUS:

```
VENDOR IBM 211
ATTRIBUTE      User-Name          1          serie
ATTRIBUTE      User-Password       2          serie
ATTRIBUTE      CHAP-Password       3          serie
ATTRIBUTE      NAS-IP-Address      4          ipaddr
ATTRIBUTE      NAS-Port            5          entero
ATTRIBUTE      Service-Type        6          entero
ATTRIBUTE      Framed-Protocol     7          entero
ATTRIBUTE      Framed-IP-Address   8          ipaddr
ATTRIBUTE      Framed-IP-Netmask   9          ipaddr
ATTRIBUTE      Framed-Routing      10         entero
ATTRIBUTE      Filter-Id           11         serie
ATTRIBUTE      Framed-MTU          12         entero
ATTRIBUTE      Framed-Compression  13         entero
ATTRIBUTE      Login-IP-Host       14         ipaddr
ATTRIBUTE      Login-Service       15         entero
ATTRIBUTE      Login-TCP-Port      16         núm. entero
ATTRIBUTE      Old-Password        17         serie
ATTRIBUTE      Reply-Message       18         serie
ATTRIBUTE      Callback-Number     19         serie
ATTRIBUTE      Callback-Id        20         núm. serie
ATTRIBUTE      Unassigned          21         serie
ATTRIBUTE      Framed-Route        22         serie
ATTRIBUTE      Framed-IPX-Network  23         entero
ATTRIBUTE      State               24         serie
ATTRIBUTE      Class               25         serie
ATTRIBUTE      Vendor-Specific     26         serie
ATTRIBUTE      Session-Timeout     27         entero
ATTRIBUTE      Idle-Timeout        28         entero
ATTRIBUTE      Termination-Action  29         entero
ATTRIBUTE      Called-Station-Id   30         serie
ATTRIBUTE      Calling-Station-Id  31         serie
ATTRIBUTE      NAS-Identifier       32         serie
ATTRIBUTE      Proxy-State         33         serie
ATTRIBUTE      Login-LAT-Service   34         serie
ATTRIBUTE      Login-LAT-Node      35         serie
ATTRIBUTE      Login-LAT-Group     36         serie
ATTRIBUTE      Framed-Appletalk-Link 37         entero
ATTRIBUTE      Framed-Appletalk-Net 38         entero
ATTRIBUTE      Framed-Appletalk-Zone 39         serie
ATTRIBUTE      Acct-Status-Type    40         entero
ATTRIBUTE      Acct-Delay-Time     41         entero
ATTRIBUTE      Acct-Input-Octets   42         entero
ATTRIBUTE      Acct-Output-Octets  43         entero
ATTRIBUTE      Acct-Session-Id     44         serie
ATTRIBUTE      Acct-Authentic      45         entero
ATTRIBUTE      Acct-Session-Time   46         entero
ATTRIBUTE      Acct-Input-Packets  47         entero
ATTRIBUTE      Acct-Output-Packets 48         entero
ATTRIBUTE      Acct-Terminate-Cause 49         entero
ATTRIBUTE      Acct-Multi-Session-Id 50         serie
ATTRIBUTE      Acct-Link-Count     51         entero
```

ATTRIBUTE	CHAP-Challenge	60	serie
ATTRIBUTE	NAS-Port-Type	61	entero
ATTRIBUTE	Port-Limit	62	entero
ATTRIBUTE	Login-LAT-Port	63	serie
----- START IBM -----			
ATTRIBUTE	Tunnel-Type	64	entero
ATTRIBUTE	Tunnel-Medium	65	entero
ATTRIBUTE	Tunnel-Client-EP	66	serie
ATTRIBUTE	Tunnel-Server-EP	67	serie
ATTRIBUTE	Tunnel-Conn-ID	68	serie
ATTRIBUTE	Tunnel-Password	69	serie
ATTRIBUTE	Tunnel-NAS-Password	101	serie
ATTRIBUTE	VC-ACTIVE	177	entero
ATTRIBUTE	VC-IDLETIME	179	entero
ATTRIBUTE	VC-SUSPENDTIME	180	entero
ATTRIBUTE	IBM-Callback-Flags	210	serie
ATTRIBUTE	IBM-Encryption	211	serie
ATTRIBUTE	IBM-DialOut	214	serie
ATTRIBUTE	IBM-Hostname	213	serie
ATTRIBUTE	IBM-Subnetmask	215	serie
ATTRIBUTE	IBM-Privilege	216	serie
ATTRIBUTE	IBM-ipsec-inb-ah	110	entero
ATTRIBUTE	IBM-ipsec-inb-esp	111	entero
ATTRIBUTE	IBM-ipsec-ob-ah	112	entero
ATTRIBUTE	IBM-ipsec-ob-esp	113	entero
ATTRIBUTE	IBM-ipsec-ip-bad	114	entero
ATTRIBUTE	IBM-ipsec-op-bad	115	entero
ATTRIBUTE	IBM-ipsec-ip-bad-ah	116	entero
ATTRIBUTE	IBM-ipsec-ip-bad-esp	117	entero
ATTRIBUTE	IBM-ipsec-op-bad-ah	118	entero
ATTRIBUTE	IBM-ipsec-op-bad-esp	119	entero
ATTRIBUTE	IBM-ipsec-ip-ah	120	entero
ATTRIBUTE	IBM-ipsec-ip-esp	121	entero
ATTRIBUTE	IBM-ipsec-op-ah	122	entero
ATTRIBUTE	IBM-ipsec-op-esp	123	entero
ATTRIBUTE	IBM-ipsec-ip-bad-ah-r	124	entero
ATTRIBUTE	IBM-ipsec-ip-bad-esp-r	125	entero
ATTRIBUTE	IBM-ipsec-inb-wrap	128	entero
ATTRIBUTE	IBM-ipsec-ob-wrap	129	entero
ATTRIBUTE	IBM-ipsec-ib-ah-wrap	130	entero
ATTRIBUTE	IBM-ipsec-ib-esp-wrap	131	entero
ATTRIBUTE	IBM-ipsec-ob-ah-wrap	132	entero
ATTRIBUTE	IBM-ipsec-ob-esp-wrap	133	entero
ATTRIBUTE	IBM-ipsec-policy-name	135	serie
ATTRIBUTE	IBM-ipsec-p1-id	136	serie
ATTRIBUTE	IBM-ipsec-p1-name	143	serie
ATTRIBUTE	IBM-ipsec-esp-algo	140	serie
ATTRIBUTE	IBM-ipsec-ah-algo	141	serie
ATTRIBUTE	IBM-ipsec-esp-algo	142	serie
VALUE	Tunnel-Type	L2TP	3
VALUE	Tunnel-Type	L2F	2
VALUE	Tunnel-Type	PPTP	1
VALUE	Tunnel-Medium	IP	1
VALUE	VC-ACTIVE	YES	1

VALUE	VC-ACTIVE	NO	0
VALUE	IBM-Callback-Flags	Required	REQ
VALUE	IBM-Callback-Flags	Roaming	OAM
VALUE	IBM-Dialout	Enable	TRUE
VALUE	IBM-Dialout	Disable	FALSE
VALUE	IBM-Dialout	ONLY	ONLY
VALUE	IBM-Privilege	Administrator	ADMIN
VALUE	IBM-Privilege	Operator	OPER
VALUE	IBM-Privilege	Monitor	MONITOR

TACACS+

Autenticación

Autorización

Servicio PPP=ppp protocolo=ip
 Servicio LOGIN=shell cmd=null pri_lvl*0

TACACS estándar+ Atributos

service
 protocol
 cmd
 addr
 timeout
 priv_lvl 0 (privilegio de supervisor),
 1 (privilegio de operador),
 15 (privilegio de administrador)
 callback-dialstring

Atributos específicos de IBM

encryption_key 16 caracteres hexadecimales
 dial_out TRUE FALSE ONLY

Contabilidad

task_id
 start_time
 stop_time
 elapsed_time
 timezone
 event
 reason
 bytes
 bytes_in
 bytes_out
 paks
 paks_in
 paks_out
 status
 err_msg

Lista de Abreviaturas

AARP	AppleTalk Address Resolution Protocol
ABR	Direccionador de marco de área
ack	Acuse de recibo
AIX	Advanced Interactive Executive
AMA	Direccionamiento del MAC arbitrario
AMP	Supervisor presente activo
ANSI	American National Standards Institute
AP2	AppleTalk Phase 2
APPN	Advanced Peer-to-Peer Networking
ARE	Explorador de todas las rutas
ARI	Interfaz ATM real
ARI/FCI	Indicador de dirección reconocida/indicador de trama copiada
ARP	Address Resolution Protocol
AS	Sistema autónomo
ASBR	Direccionador de límite de sistema autónomo
ASCII	American National Standard Code for Information Interchange
ASN.1	Notación de sintaxis de abstracción 1
ASRT	Direccionamiento transparente de origen adaptable
ASYNC	Asíncrono
ATCP	AppleTalk Control Protocol
ATP	AppleTalk Transaction Protocol
AUI	Interfaz de unidad de conexión
AVI	Interfaz ATM virtual
ayt	¿Hay alguien ahí?
BAN	Boundary Access Node
BBCM	Bridging Broadcast Manager
BECN	Notificación de congestión explícita hacia atrás
BGP	Border Gateway Protocol
BNC	Bayonet Niell-Concelman
BNCP	Bridging Network Control Protocol
BOOTP	Protocolo BOOT
BPDU	Unidad de datos de protocolo de puente
bps	Bits por segundo
BR	Función de puente/direccionamiento

BRS Reserva de ancho de banda

BSD Distribución de software de Berkeley

BTP Agente de relay de BOOTP

BTU Unidad básica de transmisión

CAM Memoria dirigible a través del contenido

CCITT Comisión Consultiva de la Telefonía y Telegrafía Internacionales

CD Detección de colisión

CGWCON
Consola de pasarela

CIDR Direccionamiento entre dominios sin clase

CIP Classical IP

CIR Velocidad de información comprometida

CLNP Connectionless-Mode Network Protocol

CPU Unidad central de proceso

CRC Comprobación de redundancia cíclica

CRS Servidor de informes de configuración

CTS Preparado para transmitir

CUD Datos de usuario de llamada

DAF Filtración de direcciones de destino

DB Base de datos

DBsum
Resumen de la base de datos

DCD Detector de señal de línea recibida de canal de datos

DCE Equipo de terminación de circuito de datos

DCS Servidor conectado directamente

DDLC Controlador de enlace de datos dual

DDN Defense Data Network

DDP Datagram Delivery Protocol

DDT Dynamic Debugging Tool

DHCP Dynamic Host Configuration Protocol

dir Conectado directamente

DL Enlace de datos

DLC Control de enlace de datos

DLCI Identificador de conexión de enlace de datos

DLS Conmutación del enlace de datos

DLSw Conmutación del enlace de datos

DMA Acceso de memoria directo

DNA Digital Network Architecture

DNCP	DECnet Protocol Control Protocol
DNIC	Código de identificador de red de datos
DdD	Departamento de Defensa
DOS	Disk Operating System
DR	Direccionador designado
DRAM	Memoria de acceso aleatorio dinámica
DSAP	Punto de acceso a servicios de destino
DSE	Equipo de conmutación de datos
DSE	Intercambio de conmutaciones de datos
DSR	Aparato de datos preparado
DSU	Unidad de servicio de datos
DTE	Equipo terminal de datos
DTR	Terminal de datos preparado
Dtype	Tipo de destino
DVMRP	Distance Vector Multicast Routing Protocol
E&M	Ear & Mouth
E1	Velocidad de transmisión de 2,048 Mbps
EDEL	Delimitador de final
EDI	Indicador de errores detectados
EGP	Exterior Gateway Protocol
EIA	Electronics Industries Association
ELAN	LAN emulada
ELAP	EtherTalk Link Access Protocol
ELS	Sistema de anotación cronológica de sucesos
ELSCon	Consola secundaria de ELS
ESI	Identificador de sistema final
EST	Horario Estándar del Este de los EE.UU
Eth	Ethernet
fa-ga	Dirección funcional-dirección de grupo
FCS	Secuencia de comprobación de trama
FECN	Notificación de congestión explícita hacia adelante
FIFO	Primero en entrar, primero en salir
FLT	Biblioteca de filtros
FR	Frame Relay
FRL	Frame Relay
FTP	File Transfer Protocol

FXO	Foreign Exchange Office
FXS	Foreign Exchange Station
GMT	Hora Media de Greenwich
GOSIP	Perfil de Interconexión de Sistemas Abiertos del Gobierno
GTE	Compañía Telefónica General
GWCON	Consola de pasarela
HDLC	Control de enlace de datos de alto nivel
HEX	Hexadecimal
HPR	Direccionamiento de alto rendimiento
HST	Servicios de sistema principal de TCP/IP
HTF	Formato de tabla de sistema principal
IBD	Dispositivo de arranque integrado
ICMP	Internet Control Message Protocol
ICP	Internet Control Protocol
ID	Identificación
IDP	Parte de dominio inicial
IDP	Internet Datagram Protocol
IEEE	Institute of Electrical and Electronics Engineers
Ifc#	Número de interfaz
IGP	Interior Gateway Protocol
InARP	Inverse Address Resolution Protocol
IP	Internet Protocol
IPCP	IP Control Protocol
IPPN	IP Protocol Network
IPX	Internetwork Packet Exchange
IPXCP	IPX Control Protocol
RDSI	Red digital de servicios integrados
ISO	Organización Internacional para la Normalización
Kbps	Kilobits por segundo
LAC	Concentrador del acceso a la red L2TP
LAN	Red de área local
LAPB	Protocolo de acceso a enlace equilibrado
LAT	Transporte de área local
LCS	Estación de canal de LAN
LCP	Link Control Protocol
LED	Diodo emisor de luz

LF	Trama mayor; salto de línea
LIS	Subred IP lógica
LLC	Control de enlace lógico
LLC2	Control de enlace lógico 2
LMI	Interfaz de gestión local
LNS	Servidor de red L2TP
LRM	Mecanismo de información de LAN
LS	Estado de los enlaces
LSA	Notificación del estado de los enlaces
LSA	Link Services Architecture
LSB	Bit menos significativo
LSI	Interfaz de métodos abreviados de LAN
LSreq	Petición del estado de los enlaces
LSrxl	Lista de retransmisiones del estado de los enlaces
LU	Unidad lógica
MAC	Control del acceso al medio
Mb	Megabit
MB	Megabyte
Mbps	Megabits por segundo
MBps	Megabytes por segundo
MC	Multidifusión
MCF	Filtro del MAC
MIB	Base de la información de gestión
MIB II	Base de la información de gestión II
MILNET	Red militar
MOS	Micro Operating System
MOSDBG	Micro Operating System Debugging Tool
MOSPF	Open Shortest Path First con extensiones de multidifusión
MPC	Canal de diversas vías de acceso
MPC+	Canal de diversas vías de acceso de transferencia de datos de alto rendimiento (HPDT)
MSB	Bit más significativo
MSDU	Unidad de datos de servicio MAC
MRU	Unidad máxima de recepción
MTU	Unidad máxima de transmisión
nak	Sin acuse de recibo

NAS Estación Nways Switch Administration

NBMA Acceso múltiple sin difusión

NBP Name Binding Protocol

NBR Direccionador contiguo

NCP Network Control Protocol

NCP Network Core Protocol

NDPS Conmutación de vías de acceso sin interrupciones

NetBIOS
Network Basic Input/Output System

NHRP Next Hop Resolution Protocol

NIST National Institute of Standards and Technology

NPDU Unidad de datos de protocolo de red

NRZ Sin vuelta a cero

NRZI Sin vuelta a cero invertido

NSAP Punto de acceso a servicios de red

NSF National Science Foundation

NSFNET
National Science Foundation NETwork

NVCNFG
Configuración permanente

OOS Fuera de servicio

OPCON
Consola del operador

OSI Interconexión de sistemas abiertos

OSICP
OSI Control Protocol

OSPF Open Shortest Path First

OUI Identificador exclusivo de organización

PC Personal Computer

PCA Adaptador de canal paralelo

PCR Velocidad mayor de célula

PDN Red de datos pública

PING Sonda de paquetes InterNet

PDU Unidad de datos de protocolo

PID Identificación de proceso

P-P Point-to-Point

PPP Point-to-Point Protocol

PROM Memoria de sólo lectura programable

PU Unidad física

PVC	Circuito virtual permanente
RAM	Memoria de acceso aleatorio
RD	Descriptor de ruta
REM	Supervisor de errores de anillo
REV	Recepción
RFC	Request for Comments
RI	Indicador de llamada; información de direccionamiento
RIF	Campo de información de direccionamiento
RII	Indicador de información de direccionamiento
RIP	Routing Information Protocol
RISC	Sistema de juego reducido de instrucciones
RNR	Recepción no preparada
ROM	Memoria de sólo lectura
ROpcon	Consola del operador remota
RPS	Servidor de parámetros de anillo
RTMP	Routing Table Maintenance Protocol
RTP	RouTing update Protocol
RTS	Petición de emisión
Rtype	Tipo de ruta
rxmits	Retransmisiones
rxmt	Retransmisión
s	Segundo
SAF	Filtración de direcciones de origen
SAP	Punto de acceso a servicios
SAP	Service Advertising Protocol
SCR	Velocidad sostenida de célula
SCSP	Server Cache Synchronization Protocol
sdel	Delimitador de inicio
SDLC	Relay de SDLC, control síncrono de enlace de datos
seqno	Número de secuencia
SGID	Identificación de grupo de servidores
SGMP	Simple Gateway Monitoring Protocol
SL	Línea serie
SMP	Supervisor presente en espera
SMTP	Simple Mail Transfer Protocol
SNA	Systems Network Architecture
SNAP	Subnetwork Access Protocol

SNMP	Simple Network Management Protocol
SNPA	Punto de conexión de subred
SPF	Ruta intraárea OSPF
SPE1	Tipo 1 de ruta externa OSPF
SPE2	Tipo 2 de ruta externa OSPF
SPIA	Tipo de ruta interárea OSPF
SPID	Identificación de perfil de servicio
SPX	Sequenced Packet Exchange
SQE	Error en calidad de señal
SRAM	Memoria de acceso aleatorio estática
SRB	Puente de direccionamiento de origen
SRF	Trama específicamente direccionada
SRLY	Relay de SDLC
SRT	Direccionamiento transparente de origen
SR-TB	Puente de direccionamiento transparente de origen
STA	Estático
STB	Puente de árbol de expansión
STE	Explorador de árbol de expansión
STP	Par trenzado y apantallado; protocolo de árbol de expansión
SVC	Circuito virtual conmutado
TB	Puente transparente
TCN	Notificación de cambio de topología
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TEI	Identificador de punto de terminal
TFTP	Trivial File Transfer Protocol
TKR	Red en Anillo
TMO	Tiempo de espera excedido
TOS	Tipo de servicio
TSF	Tramas de expansión transparentes
TTL	Período de duración
TTY	Teletipo
TX	Transmisión
UA	Acuse de recibo sin número
UDP	User Datagram Protocol
UI	Información sin número

UTP	Par trenzado y no apantallado
VCC	Conexión de canal virtual
VINES	Virtual NEtworking System
VIR	Velocidad de información variable
VL	Enlace virtual
VNI	Virtual Network Interface
VoFR	Voz a través de Frame Relay
VR	Ruta virtual
WAN	Red de área amplia
WRS	Redireccionamiento/restauración de WAN
X.25	Redes de paquetes conmutados
X.251	Capa física de X.25
X.252	Capa de trama de X.25
X.253	Capa de paquetes de X.25
XID	Identificación de intercambio
XNS	Xerox Network Systems
XSUM	Suma de comprobación
ZIP	AppleTalk Zone Information Protocol
ZIP2	AppleTalk Zone Information Protocol 2
ZIT	Tabla de información de zonas

Glosario

Este glosario incluye términos y definiciones de la documentación siguiente:

- El *American National Standard Dictionary for Information Systems*, ANSI X3.172-1990, copyright 1990 del American National Standards Institute (ANSI). Los ejemplares pueden adquirirse en el American National Standards Institute, 11 West 42nd Street, New York, New York 10036. Las definiciones se identifican mediante el símbolo (A) que aparece después de la definición.
- La *Norma ANSI/EIA 440-A de la Fiber Optic Terminology*. Los ejemplares pueden adquirirse en la Electronic Industries Association, 2001 Pennsylvania Avenue, N.W., Washington, DC 20006. Las definiciones se identifican mediante el símbolo (E) que aparece después de la definición.
- El *Information Technology Vocabulary* desarrollado por la Subcomisión 1, Comisión Técnica Mixta 1, de la Organización Internacional para la Normalización y la Comisión Electrotécnica Internacional (JTC1/SC1 de la ISO/IEC). Las definiciones de las secciones publicadas de este vocabulario se identifican mediante el símbolo (I) que aparece después de la definición; las definiciones de los borradores de normas internacionales, borradores de comisiones y documentos de trabajo que está desarrollando la JTC1/SC1 de la ISO/IEC se identifican mediante el símbolo (T) que aparece después de la definición, símbolo que indica que las Corporaciones Nacionales de la SC1 participantes todavía no han llegado a un acuerdo definitivo.
- El *IBM Dictionary of Computing*, New York: McGraw-Hill, 1994.
- Internet Request for Comments: 1208, *Glossary of Networking Terms*
- Internet Request for Comments: 1392, *Internet Users' Glossary*
- El *Object-Oriented Interface Design: IBM Common User Access Guidelines*, Carmel, Indiana: Que, 1992.

En este glosario, se utilizan las siguientes referencias cruzadas:

Compárese con:

Se refiere a un término que tiene un significado opuesto o esencialmente distinto.

Sinónimo de:

Indica que el término tiene el mismo significado que un término preferente, el cual está definido en el lugar que le corresponde dentro del glosario.

Sinónimo con:

Es una referencia hacia atrás de un término definido a los otros términos que tienen el mismo significado.

Véase:

Remite al lector a términos de diversas palabras que tienen la misma palabra al principio.

Véase también:

Remite al lector a términos que tienen un significado relacionado, pero no sinónimo.

A

AAL-5. Capa de adaptación de ATM 5, una de las diversas AAL estándares. AAL-5 se ha diseñado para las comunicaciones de datos y la utilizan la Emulación de LAN y el IP clásico.

AAL. Capa de adaptación de ATM, que es la que adapta los datos de usuario a/de la red ATM añadiendo/eliminando cabeceras y segmentando/volviendo a ensamblar los datos en/a partir de células.

acceso de memoria directo (DMA). Recurso del sistema que permite que un dispositivo del bus Micro Channel obtenga acceso directo a la memoria del sistema o a la memoria del bus sin la intervención del procesador del sistema.

acceso múltiple con detección de portadora y detección de colisión (CSMA/CD). Protocolo que necesita detección de portadora y en el que una estación de datos transmisora que detecta otra señal mientras transmite detiene la emisión, envía una señal de atasco y luego espera durante un período variable antes de volver a intentar la acción. (T) (A)

ACCESS. En el protocolo Simple Network Management Protocol (SNMP), cláusula de un módulo de la Base de la información de gestión (MIB) que define el nivel mínimo de soporte que proporciona un nodo gestionado para un objeto.

activo. (1) Operativo. (2) Perteneciente a un nodo o dispositivo que está conectado o está disponible para la conexión con otro nodo o dispositivo.

actualización de base de datos de topología (TDU).

Mensaje sobre un nodo o enlace nuevo o modificado que se difunde entre los nodos de red APPN para mantener la base de datos de topología de red, que está reproducida en su totalidad en cada nodo de red. Una TDU contiene información para identificar lo siguiente:

- El nodo emisor.
- Las características de nodo y enlace de diversos recursos de la red.
- El número de secuencia de la actualización más reciente para cada uno de los recursos descritos.

acuse de recibo. (1) Transmisión, por parte de un receptor, de caracteres de acuse de recibo como respuesta afirmativa a un remitente. (T) (2) Indicación de que se ha recibido un elemento enviado.

Address Resolution Protocol (ARP). (1) En el conjunto de protocolos de Internet, protocolo que correlaciona dinámicamente una dirección IP con una dirección utilizada por una red de área metropolitana o local de soporte, como, por ejemplo, Ethernet o Red en Anillo. (2) Véase también *Reverse Address Resolution Protocol (RARP)*.

Advanced Peer-to-Peer Networking (APPN).

Extensión de SNA que ofrece (a) un control superior de las redes distribuidas que evita las dependencias jerárquicas críticas y, por lo tanto, aísla los efectos de puntos anómalos individuales; (b) intercambio dinámico de información de topología de red para facilitar la conexión, reconfiguración y selección de rutas adaptables; (c) definición dinámica de recursos de red; y (d) automatización en el registro de recursos y la búsqueda en directorios. APPN hace extensiva la orientación de igual de la LU 6.2 para los servicios de usuario final al control de redes y da soporte a diversos tipos de LU, incluidas la LU 2, la LU 3 y la LU 6.2.

agencia operativa privada reconocida (RPOA).

Cualquier individuo, empresa o corporación (que no sea un departamento o servicio del gobierno) que realiza operaciones en un servicio de telecomunicaciones y está sujeta a las obligaciones definidas en el Convenio de la unión de telecomunicaciones internacionales y en la legislación; por ejemplo, una empresa de telecomunicación.

agente. Sistema que asume un papel de agente.

alerta. Mensaje enviado a un punto focal de servicios de gestión de una red para identificar un problema o un problema inminente.

American National Standards Institute (ANSI).

Organización compuesta por productores, clientes y grupos con intereses generales que establece los

procedimientos mediante los cuales organizaciones acreditadas crean y mantienen normas voluntarias de la industria en los Estados Unidos. (A)

analógico. (1) Perteneciente a datos compuestos por cantidades físicas continuamente variables. (A) (2) Compárese con *digital*.

ancho de banda. El ancho de banda de un enlace óptico designa la capacidad de contener información del enlace y está relacionado con la máxima velocidad en bits a la que puede dar soporte un enlace de fibra.

anillo. Véase *red de tipo anillo*.

anomalía en la autenticación. En el protocolo Simple Network Management Protocol (SNMP), detección (de condición de excepción) que una entidad de autenticación puede haber generado cuando un cliente peticionario no es miembro de la comunidad de SNMP.

antememoria. (1) Almacenamiento intermedio de fines especiales más pequeño y rápido que el almacenamiento principal; se utiliza para que contenga una copia de instrucciones y datos obtenidos del almacenamiento principal y que probablemente necesitará a continuación el procesador. (T) (2) Almacenamiento intermedio que contiene instrucciones y datos a los que se accede frecuentemente; se utiliza para reducir el tiempo del acceso. (3) Parte opcional de la base de datos de directorios existente en los nodos de red donde puede almacenarse información de directorios de uso frecuente para acelerar las búsquedas en directorios. (4) Colocar, ocultar o almacenar en antememoria.

aparato de datos preparado (DSR). Sinónimo de *DCE preparado*.

AppleTalk. Protocolo de red desarrollado por Apple Computer, Inc. Este protocolo se utiliza para la interconexión de dispositivos de red, que pueden ser una mezcla de productos Apple y productos que no son Apple.

AppleTalk Address Resolution Protocol (AARP). En redes AppleTalk, protocolo que (a) convierte las direcciones de nodo AppleTalk en direcciones de hardware y (b) soluciona las discrepancias de direccionamiento en las redes que dan soporte a más de un conjunto de protocolos.

AppleTalk Transaction Protocol (ATP). En redes AppleTalk, protocolo que proporciona funciones de petición y respuesta de cliente/servidor a los sistemas principales que acceden al protocolo Zone Information Protocol (ZIP) para la información de zonas.

árbol de expansión. En contextos de LAN, método mediante el cual los puentes desarrollan automáticamente una tabla de direccionamiento y actualizan esta tabla en respuesta a un cambio de la topología para asegurarse de la existencia de una sola

ruta entre dos LAN cualesquiera en la red con puentes. Este método evita bucles de paquetes, donde un paquete vuelve en una ruta de circuito al direccionador emisor.

archivo de configuración. Archivo que especifica las características de un dispositivo del sistema o una red.

área. En los protocolos de direccionamiento de Internet y DECnet, subconjunto de una red o pasarela que se ha agrupado por definición del administrador de red. Cada área es independiente; la información sobre la topología de un área permanece oculta respecto a las otras áreas.

arquitectura de red. Estructura lógica y principios operativos de una red de sistema. (T)

Nota: Los principios operativos de una red incluyen los principios de los servicios, funciones y protocolos.

arquitectura interconexión de sistemas abiertos (OSI). Arquitectura de red que se ajusta al conjunto particular de normas ISO relacionado con interconexión de sistemas abiertos. (T)

arreglo temporal del programa (PTF). Solución o ajuste temporal de un problema diagnosticado por IBM de un release actual no modificado del programa.

asequibilidad. Capacidad de un nodo o recurso para comunicarse con otro nodo o recurso.

asíncrono (ASYNC). Perteneciente a dos o más procesos que no dependen de la aparición de sucesos específicos, como, por ejemplo, señales comunes de temporización. (T)

ATM. Asynchronous Transfer Mode, tecnología de red de gran velocidad orientada a las conexiones que se basa en la conmutación de células.

ATMARP. ARP en Classical IP.

B

base de datos de configuración (CDB). Base de datos que almacena los parámetros de configuración de uno o diversos dispositivos. Se prepara y actualiza utilizando el programa de configuración.

base de la información de gestión (MIB). (1) Conjunto de objetos a los que se puede acceder por medio de un protocolo de gestión de red. (2) Definición de información de gestión que especifica la información disponible de un sistema principal o una pasarela y las operaciones permitidas. (3) En OSI, depósito conceptual de información de gestión dentro de un sistema abierto.

baudio. En la transmisión asíncrona, unidad de velocidad de modulación correspondiente al intervalo de una unidad por segundo; es decir, si la duración del intervalo de la unidad es de 20 milisegundos, la velocidad de modulación es de 50 baudios. (A)

bit D. Bit de confirmación de entrega. En comunicaciones X.25, bit de un paquete de datos o paquete de petición de llamada que se establece en 1 si el destinatario necesita acuse de recibo (confirmación de entrega) de extremo a extremo.

Border Gateway Protocol (BGP). Protocolo de direccionamiento de Internet Protocol (IP) utilizado entre dominios y sistemas autónomos.

bucle de direccionamiento. Situación que ocurre cuando los direccionadores hacen circular información entre ellos hasta que se produce la convergencia o hasta que se consideran inasequibles las redes implicadas.

C

cabecera. (1) Información de control definida por el sistema que precede a los datos de usuario. (2) Parte de un mensaje que contiene información de control para el mismo, como, por ejemplo, uno o más campos de destino, el nombre de la estación de origen, el número de secuencia de entrada, una serie de caracteres que indica el tipo de mensaje y el nivel de prioridad del mensaje.

cabecera de transmisión (TH). Información de control, seguida opcionalmente de una unidad básica de información (BIU) o de un segmento de BIU, que crea y utiliza el control de la vía de acceso para direccionar unidades de mensajes y controlar su flujo dentro de la red. Véase también *unidad de información de vía de acceso*.

canal. (1) Vía de acceso por la que pueden enviarse señales, como, por ejemplo, canal de datos, canal de salida. (A) (2) Unidad funcional, controlada por el procesador, que maneja la transferencia de datos entre el almacenamiento del procesador y el equipo de periféricos local.

canal de diversas vías de acceso (MPC). Protocolo de canal que utiliza diversos subcanales unidireccionales para la comunicación bidireccional de VTAM a VTAM.

canal de entrada/salida. En un sistema de proceso de datos, unidad funcional que maneja la transferencia de datos entre el equipo interno y el equipo de periféricos. (I) (A)

canalización. Proceso consistente en romper el ancho de banda de una línea de comunicaciones en varios

canales, posiblemente de diferentes tamaños. También se denomina **multiplexación de la división del tiempo** (TDM).

canal lógico. En el funcionamiento en modalidad de paquete, canal de emisión y canal de recepción que se utilizan conjuntamente para enviar y recibir datos sobre un enlace de datos al mismo tiempo. Pueden establecerse varios canales lógicos en el mismo enlace de datos si se interpone la transmisión de paquetes.

capa. (1) En una arquitectura de red, grupo de servicios que está completo desde un punto de vista conceptual, que es uno de los grupos de un conjunto de grupos ordenados jerárquicamente y que se extiende por todos los sistemas que se ajustan a la arquitectura de red. (T) (2) En el modelo de referencia interconexión de sistemas abiertos, uno de los siete grupos de servicios, funciones y protocolos ordenados jerárquicamente y completos conceptualmente que se extienden por todos los sistemas abiertos. (T) (3) En SNA, agrupación de funciones relacionadas que están separadas lógicamente de las funciones de otros grupos. La implementación de las funciones de una capa puede cambiar sin que ello afecte a las funciones de otras capas.

capa de control de enlace de datos (DLC). En SNA, capa que está compuesta por las estaciones de enlace que planifican la transferencia de datos sobre un enlace entre dos nodos y realizan un control de errores para el enlace. Ejemplos de control de enlace de datos son: el SDLC para la conexión de enlaces serie por bit y el control de enlace de datos para el canal de System/370.

Nota: Normalmente, la capa de DLC es independiente del mecanismo de transporte físico y asegura la integridad de los datos que alcanzan las capas superiores.

capa de enlace de datos. En el modelo de referencia de OSI (interconexión de sistemas abiertos), capa que proporciona servicios para la transferencia de datos entre las entidades de la capa de red sobre un enlace de comunicaciones. La capa de enlace de datos detecta los errores que puedan producirse en la capa física y posiblemente los corrige. (T)

capa de red. En la arquitectura interconexión de sistemas abiertos (OSI), capa que es responsable del direccionamiento, de la conmutación y del acceso a la capa de enlace a lo largo del entorno de OSI.

capa de transporte. En el modelo de referencia interconexión de sistemas abiertos, capa que proporciona un servicio fiable de transferencia de datos de extremo a extremo. Puede haber sistemas abiertos del tipo Relay en la vía de acceso. (T) Véase también *modelo de referencia interconexión de sistemas abiertos*.

capa física. En el modelo de referencia interconexión de sistemas abiertos, capa que proporciona los medios mecánicos, eléctricos, funcionales y de procedimiento para establecer, mantener y liberar conexiones físicas sobre el medio de transmisión. (T)

carácter comodín. Sinónimo de *carácter de coincidencia con el patrón*.

carácter de coincidencia con el patrón. Carácter especial, como, por ejemplo, un asterisco (*) o un signo de interrogación (?), que puede utilizarse para representar uno o más caracteres. Cualquier carácter o conjunto de caracteres puede sustituir a un carácter de coincidencia con el patrón. Sinónimo con *carácter global* y *carácter comodín*.

CCITT. Comisión consultiva de la telefonía y telegrafía Internacionales. Era una organización de la Unión de Telecomunicaciones Internacionales (ITU). El 1 de marzo de 1993 se reorganizó la ITU y las responsabilidades de la normalización recayeron en una organización subordinada que se denomina Sector de normalización de telecomunicaciones de la unión de telecomunicaciones (ITU-TS). La "CCITT" sigue funcionando para las recomendaciones que se aprobaron antes de la reorganización.

central privada (PBX). Central telefónica privada para la transmisión de llamadas desde y hacia la red telefónica pública.

centro de información de la red (NIC). En comunicaciones de Internet, grupos locales, regionales y nacionales de todo el mundo que proporcionan ayuda, documentación, formación y otros servicios a los usuarios.

circuito de datos. (1) Par de canales de transmisión y recepción asociados que proporcionan un medio de comunicación de datos de dos direcciones. (I) (2) En SNA, sinónimo de *conexión de enlace*. (3) Véase también *circuito físico* y *circuito virtual*.

Notas:

1. Entre los intercambios de conmutaciones de datos, el circuito de datos puede incluir un equipo de terminación de circuito de datos (DCE) de acuerdo con el tipo de interfaz que se utilice en el intercambio de conmutaciones de datos.
2. Entre una estación de datos y un intercambio de conmutaciones de datos o concentrador de datos, el circuito de datos incluye el equipo de terminación de circuito de datos en el extremo de la estación de datos y puede incluir un equipo similar a un DCE en el intercambio de conmutaciones de datos o en la ubicación del concentrador de datos.

circuito físico. Circuito establecido sin multiplexación. Véase también *circuito de datos*. Compárese con *circuito virtual*.

circuito huérfano. Circuito no configurado cuya disponibilidad se aprende dinámicamente.

circuito virtual. (1) En la conmutación de paquetes, recursos proporcionados por una red que ofrecen el aspecto de una conexión real ante el usuario. (T) Véase también *circuito de datos*. Compárese con *circuito físico*. (2) Conexión lógica establecida entre dos DTE.

circuito virtual conmutado (SVC). Circuito X.25 que se establece dinámicamente cuando es necesario. El equivalente, en X.25, de una línea conmutada. Compárese con *circuito virtual permanente (PVC)*.

circuito virtual permanente (PVC). En comunicaciones de X.25 y Frame-Relay, circuito virtual que tiene un canal lógico asignado permanentemente al mismo en cada equipo terminal de datos (DTE). No son necesarios protocolos de establecimiento de llamada. Compárese con *circuito virtual conmutado (SVC)*.

clase de productividad. En la conmutación de paquetes, velocidad a la que circulan los paquetes de un equipo terminal de datos (DTE) por la red de conmutación de paquetes.

clase de servicio (COS). Conjunto de características (como, por ejemplo, seguridad de ruta, prioridad de transmisión y ancho de banda) utilizadas para crear una ruta entre los asociados a una sesión. La clase de servicio deriva de un nombre de modalidad especificado por el iniciador de una sesión.

cliente. (1) Unidad funcional que recibe servicios compartidos de un servidor. (T) (2) Usuario.

cliente de emulación de LAN (LEC). Componente de la emulación de LAN que representa a los usuarios de la LAN emulada.

cliente/servidor. En comunicaciones, modelo de interacción en el proceso de datos distribuidos en el que un programa de un sitio envía una petición a un programa de otro sitio y espera una respuesta. El programa peticionario se denomina cliente; el programa que responde se denomina servidor.

codificar. Convertir datos mediante el uso de un código de manera que sea posible la reconversión al formato original. (T)

colisión. Condición no deseada que deriva de la existencia de transmisiones simultáneas en un canal. (T)

compresión. (1) Proceso consistente en eliminar claros, campos vacíos, redundancias y datos innecesarios para disminuir la longitud de los registros o los bloques. (2) Cualquier codificación destinada a reducir el número de bits utilizados para representar un mensaje o un registro determinado.

comunidad. En el protocolo Simple Network Management Protocol (SNMP), relación administrativa entre las entidades.

Concentrador del acceso a L2TP (LAC). Dispositivo conectado a una o más líneas RDSI o de red telefónica de servicios públicos (PSTN) con posibilidades de manejar el funcionamiento de PPP y el del protocolo L2TP. El LAC implementa el medio sobre el que funciona L2TP. L2TP pasa el tráfico a uno o más Servidores de red L2TP (LNS). L2TP puede proporcionar la función de túnel para cualquier protocolo que conlleve la red PPP.

concentrador (inteligente). Concentrador de cableado, como, por ejemplo, el IBM 8260, que proporciona funciones de puente y direccionamiento a las LAN con diferentes cables y protocolos.

conectable en caliente. Se refiere a un componente de hardware que puede instalarse o eliminarse sin estorbar el funcionamiento de otros recursos que no están conectados a este componente o no dependen del mismo.

conectado mediante enlace. (1) Perteneciente a dispositivos que están conectados a una unidad de control por medio de un enlace de datos. (2) Compárese con *conectado mediante canal*. (3) Sinónimo con *remoto*.

conexión. En la comunicación de datos, asociación establecida entre unidades funcionales para comunicar información. (I) (A)

conexión de enlace. (1) Equipo físico que proporciona comunicación en dos direcciones entre una estación de enlace y otra u otras estaciones de enlace; por ejemplo, un equipo de terminación de circuito de datos (DCE) y una línea de telecomunicaciones. (2) En SNA, sinonimia con *circuito de datos*.

conexión Rapid Transport Protocol (RTP). En el direccionamiento de alto rendimiento (HPR), conexión establecida entre los puntos finales de la ruta para transportar tráfico de sesión.

conexión virtual. En Frame Relay, vía de acceso de vuelta de una conexión potencial.

configuración. (1) Manera en que están organizados e interconectados el hardware y el software de un sistema de proceso de información. (T) (2) Dispositivos y programas que componen un sistema, un subsistema o una red.

configuración del sistema. Proceso que especifica los dispositivos y programas que componen un sistema de proceso de datos determinado.

congestión. Véase *congestión de la red*.

congestión de la red. Condición no deseada de carga excesiva causada por la presencia de más tráfico del que puede manejar una red.

conmutación de la línea. Sinónimo de *conmutación del circuito*.

conmutación del circuito. (1) Proceso que, a petición, conecta dos o más equipos terminales de datos (DTE) y permite el uso exclusivo de un circuito de datos entre ellos hasta que se libera la conexión. (1) (A) (2) Sinónimo con *conmutación de la línea*.

conmutación del enlace de datos (DLSw). Método para transportar protocolos de red que utilizan el tipo 2 de control de enlace lógico (LLC) de IEEE 802.2. SNA y NetBIOS son ejemplos de protocolos que utilizan el tipo 2 de LLC. Véase también *encapsulación y simulación*.

conmutación de paquetes. (1) Proceso consistente en direccionar y transferir datos por medio de paquetes dirigidos de manera que un canal esté ocupado durante la transmisión de un paquete solamente. Cuando se completa la transmisión, el canal queda disponible para la transferencia de otros paquetes. (1) (2) Sinónimo con *funcionamiento en modalidad de paquete*. Véase también *conmutación del circuito*.

consola remota. Estación que ejecuta OS/2, TCP/IP y el programa Nways Switch Resource Control remoto. Puede conectarse con cualquier estación de soporte de red para realizar operaciones en Nways Switch y darle servicio técnico remotamente.

La conexión puede ser mediante:

- Una línea conmutada que utilice un módem

Cualquier estación de soporte de red puede utilizarse como consola remota de otra estación de soporte de red.

contigua activa de donde proceden los datos (NAUN). En la Red en Anillo de IBM, estación que envía datos directamente a una estación determinada del anillo.

control de enlace de datos de alto nivel (HDLC). En la comunicación de datos, utilización de una serie de bits especificada para controlar enlaces de datos de acuerdo con las normas internacionales respecto al HDLC: la estructura de trama de ISO 3309 y los elementos de procedimientos de ISO 4335.

control de enlace de datos (DLC). Conjunto de normas utilizado por los nodos de un enlace de datos (como, por ejemplo, un enlace de SDLC o una Red en Anillo) para efectuar un intercambio de información ordenado.

control de enlace lógico (LLC). Subcapa de LAN de control de enlace de datos (DLC) que proporciona dos tipos de operaciones de DLC para el intercambio ordenado de información. El primer tipo es el servicio

sin conexiones, que permite enviar y recibir información sin establecer un enlace. La subcapa de LLC no efectúa recuperación de errores ni control del flujo para el servicio sin conexiones. El segundo tipo es el servicio orientado a las conexiones, que requiere el establecimiento de un enlace antes del intercambio de información. El servicio orientado a las conexiones proporciona transferencia de información en secuencia, control del flujo y recuperación de errores.

control del acceso al medio (MAC). En las LAN, subcapa de la capa de control de enlace de datos que da soporte a funciones dependientes del medio y utiliza los servicios de la capa física para proporcionar servicios a la subcapa de control de enlace lógico (LLC). La subcapa del MAC incluye el método para determinar cuándo un dispositivo tiene acceso al medio de transmisión.

control de la vía de acceso (PC). Función que direcciona unidades de mensajes entre las unidades de red accesibles de la red y proporciona las vías de acceso entre éstas. Convierte las unidades básicas de información (BIU) del control de transmisión (posiblemente segmentándolas) en unidades de información de vía de acceso (PIU) e intercambia unidades básicas de transmisión que contienen una o más PIU con el control de enlace de datos. El control de la vía de acceso difiere según el tipo de nodo: algunos nodos (los nodos APPN, por ejemplo) utilizan identificadores de sesión generados localmente para el direccionamiento y otros (los nodos de subárea) utilizan direcciones de red para el direccionamiento.

control del flujo. (1) En SNA, proceso consistente en gestionar la velocidad a la que pasa el tráfico de datos entre los componentes de la red. La finalidad del control del flujo es optimizar la velocidad del flujo de unidades de mensajes con la congestión mínima de la red; es decir, ni desbordar los almacenamientos intermedios del receptor o de nodos de direccionamiento intermedio ni dejar al receptor esperando más unidades de mensajes. (2) Véase también *ritmo*.

Control síncrono de enlace de datos (SDLC). (1) Disciplina que se ajusta a los subconjuntos de los Advanced Data Communication Control Procedures (ADCCP) del American National Standards Institute (ANSI) y del High-level Data Link Control (HDLC) de la organización internacional para la normalización, y está destinada a la gestión de la transferencia síncrona de información serie por bit de código transparente sobre una conexión de enlace. Los intercambios de transmisiones pueden ser dúplex o semi-dúplex sobre enlaces conmutados o no conmutados. La configuración de la conexión de enlace puede ser de punto a punto, de multipunto o de bucle. (1) (2) Compárese con *comunicación síncrona en binario (BSC)*.

correlación. Proceso consistente en convertir datos que el emisor transmite con un formato determinado en el formato de datos que puede aceptar el receptor.

corriente de datos general (GDS). Corriente de datos utilizada para las conversaciones en sesiones de LU 6.2.

coste de la vía de acceso. En los protocolos de direccionamiento de estado de los enlaces, suma de los costes de enlace a lo largo de la vía de acceso entre dos nodos o redes.

cronometraje. (1) En la comunicación síncrona en binario, utilización de pulsaciones de reloj para controlar la sincronización de los datos y caracteres de control. (2) Método para controlar el número de bits de datos enviados en una línea de telecomunicaciones en un momento determinado.

cuenta de saltos. (1) Métrica o medida de distancia entre dos puntos. (2) En comunicaciones de Internet, número de direccionadores por los que pasa un datagrama cuando se dirige a su destino. (3) En SNA, medida consistente en el número de enlaces por los que se debe pasar en la vía de acceso a un destino.

D

daemon. Programa que se ejecuta desatendido para realizar un servicio estándar. Algunos daemon se desencadenan de manera automática para realizar su tarea; otros realizan las operaciones periódicamente.

datagrama. (1) En la conmutación de paquetes, paquete individual e independiente de otros paquetes que contiene información suficiente para el direccionamiento desde el equipo terminal de datos (DTE) de origen al DTE de destino sin apoyarse en intercambios anteriores entre los DTE y la red. (l) (2) En TCP/IP, unidad básica de información que pasa a través del entorno de Internet. Un datagrama contiene direcciones de origen y de destino junto con los datos. Un datagrama de Internet Protocol (IP) está compuesto por una cabecera de IP seguida de los datos de capa de transporte. (3) Véase también *paquete* y *segmento*.

datagrama de IP. En el conjunto de protocolos de Internet, unidad básica de información transmitida a través de una internet. Contiene direcciones de origen y de destino, datos de usuario e información de control, como, por ejemplo, la longitud del datagrama, la suma de comprobación de cabecera y distintivos que indican si el datagrama puede fragmentarse o si se ha fragmentado.

Datagram Delivery Protocol (DDP). En redes AppleTalk, protocolo que proporciona conectividad de red por medio de un servicio de entrega de socket a socket sin conexiones de la capa de internet.

DCE preparado. En la norma EIA 232, señal que indica al equipo terminal de datos (DTE) que el equipo de terminación de circuito de datos (DCE) local está conectado al canal de comunicaciones y se encuentra preparado para enviar datos. Sinónimo con *aparato de datos preparado (DSR)*.

DECnet. Arquitectura de red que define el funcionamiento de una familia de módulos de software, bases de datos y componentes de hardware que se utilizan normalmente con el fin de conectar entre sí sistemas Digital Equipment Corporation para el compartimiento de recursos, cálculo distribuido o configuración de sistemas remotos. Las implementaciones de la red DECnet siguen el modelo Digital Network Architecture (DNA).

detección de colisión. En el acceso múltiple con detección de portadora y detección de colisión (CSMA/CD), señal que indica que dos o más estaciones están transmitiendo simultáneamente.

detección (de condición de excepción). En Simple Network Management Protocol (SNMP), mensaje enviado por un nodo gestionado (la función de agente) a una estación de gestión para informarle de una condición de excepción.

detección de portadora. En una red de área local, actividad continua de una estación de datos para detectar si otra estación está transmitiendo. (T)

detector de portadora. Sinónimo de *detector de señal de línea recibida (RLSD)*.

detector de portadora de datos (DCD). Sinónimo de *detector de señal de línea recibida (RLSD)*.

detector de señal de línea recibida (RLSD). En la norma EIA 232, señal que indica al equipo terminal de datos (DTE) que está recibiendo una señal del equipo de terminación de circuito de datos (DCE) remoto. Sinónimo con *detector de portadora* y *detector de portadora de datos (DCD)*.

determinación de problemas. Proceso consistente en determinar el origen de un problema; por ejemplo, un componente de un programa, una anomalía en una máquina, recursos de telecomunicaciones, programas o equipos instalados por el contratista o por el usuario, una anomalía del entorno, como, por ejemplo, pérdida de alimentación, o un error del usuario.

difusión. (1) Transmisión de los mismos datos a todos los destinos. (T) (2) Transmisión simultánea de datos a más de un destino. (3) Compárese con *multidifusión*.

digital. (1) Perteneciente a datos compuestos por dígitos. (T) (2) Perteneciente a datos con formato de dígitos. (A) (3) Compárese con *analógico*.

Digital Network Architecture (DNA). Modelo para todas las implementaciones de hardware y software DECnet.

dirección. En la comunicación de datos, código exclusivo asignado a cada dispositivo, estación de trabajo o usuario conectado a una red.

dirección administrada localmente. En una red de área local, dirección de adaptador que el usuario puede asignar para alterar temporalmente la dirección administrada universalmente. Compárese con *dirección administrada universalmente*.

dirección administrada universalmente. En una red de área local, dirección codificada de forma permanente en un adaptador en el momento de la fabricación. Todas las direcciones administradas universalmente son exclusivas. Compárese con *dirección administrada localmente*.

direccionador. (1) Sistema que determina la vía de acceso del flujo de tráfico de red. La selección de vía de acceso se realiza entre diversas vías de acceso sobre la base de la información obtenida a partir de protocolos específicos, algoritmos que intentan identificar la vía de acceso mejor o la más corta, y otros criterios, como, por ejemplo, direcciones de destino específicas de los protocolos o la métrica. (2) Dispositivo de conexión que conecta dos segmentos de LAN, los cuales utilizan arquitecturas similares o diferentes, en la capa de red del modelo de referencia. (3) En terminología de OSI, función que determina una vía de acceso mediante la cual puede accederse a una entidad. (4) En TCP/IP, sinonimia con *pasarela*. (5) Compárese con *puente*.

direccionador contiguo. Direccionador de una subred común designado por un administrador de red para recibir información de direccionamiento.

direccionador de frontera. En comunicaciones de Internet, direccionador que está posicionado al borde de un sistema autónomo y se comunica con un direccionador que está posicionado al borde de un sistema autónomo diferente.

direccionador de germinación. En redes AppleTalk, direccionador que mantiene datos de configuración (números de red de rango y listas de zonas, por ejemplo) para la red. Cada red debe tener, como mínimo, un direccionador de germinación. El direccionador de germinación debe configurarse inicialmente por medio de la herramienta configuradora. Compárese con *direccionador sin germinación*.

direccionador de IP. Dispositivo de una internet IP que tiene la responsabilidad de tomar decisiones acerca de las vías de acceso por las que fluirá tráfico de red. Los protocolos de direccionamiento se utilizan para obtener información sobre la red y para determinar la mejor ruta por la que debe reenviarse el datagrama

hacia el destino final. Los datagramas se direccionan sobre la base de direcciones de destino IP.

direccionador designado. Direccionador que informa a los nodos finales de la existencia y la identidad de los otros direccionadores. La selección del direccionador designado se basa en el direccionador con la prioridad superior. Cuando diversos direccionadores comparten la prioridad superior, se selecciona el direccionador con la dirección de estación superior.

direccionador sin germinación. En redes AppleTalk, direccionador que obtiene información del rango de números de red y de la lista de zonas de un direccionador de germinación conectado a la misma red.

direccionador troncal. (1) Direccionador utilizado para transmitir datos entre áreas. (2) Direccionador de una serie que se utiliza para interconectar redes de manera que formen una internet mayor.

direccionamiento. En la comunicación de datos, manera que tiene una estación de seleccionar la estación a la que va a enviar datos.

direccionamiento. (1) Asignación de la vía de acceso mediante la cual un mensaje va a alcanzar su destino. (2) En SNA, reenvío de una unidad de mensaje por una vía de acceso determinada a través de una red tal como lo determinan los parámetros contenidos en la unidad de mensaje, como, por ejemplo, la dirección de red de destino de una cabecera de transmisión.

direccionamiento de alto rendimiento (HPR). Adición para la arquitectura Advanced Peer-to-Peer Networking (APPN) que mejora el rendimiento y la fiabilidad del direccionamiento de datos, especialmente en la utilización de enlaces de gran velocidad.

direccionamiento del MAC arbitrario (AMA). En la arquitectura DECnet, esquema de direccionamiento utilizado por DECnet Phase IV-Prime que da soporte a direcciones administradas universalmente y direcciones administradas localmente.

direccionamiento de origen. En las LAN, método mediante el cual la estación emisora determina la ruta que la trama seguirá e incluye la información de direccionamiento en la trama. A continuación, los puentes leen la información de direccionamiento para determinar si deben reenviar la trama.

direccionamiento de sesiones intermedias (ISR). Tipo de función de direccionamiento de un nodo de red APPN que proporciona información de indisponibilidad y control del flujo de nivel de sesión para todas las sesiones que pasan por el nodo pero cuyos puntos finales están en otra parte.

direccionamiento dinámico. Direccionar utilizando rutas aprendidas en lugar de las rutas configuradas estáticamente durante la inicialización.

direccionamiento intraárea. En comunicaciones de Internet, direccionamiento de datos dentro de un área.

dirección canónica. En las LAN, formato de IEEE 802.1 de la transmisión de direcciones del control del acceso al medio (MAC) para adaptadores de Red en Anillo y Ethernet. En el formato canónico, el bit menos significativo (situado más a la derecha) de cada byte de dirección se transmite en primer lugar. Compárese con *dirección no canónica*.

dirección de difusión. En comunicaciones, dirección de estación (ocho números 1) reservada como dirección común a todas las estaciones de un enlace. Sinónimo con *dirección de todas las estaciones*.

dirección de dispositivo. Dirección de unidad transmitida por la vía de acceso de canal para seleccionar un dispositivo 2216. También se denomina número de subcanal en la arquitectura de E/S S/370. Este valor está definido en el IOCP del sistema principal mediante la sentencia UNITADD de la instrucción de macro CNTLUNIT para el dispositivo real.

Dirección de enlace. Para el 2216 con un Adaptador de Canal ESCON, número de puerto determinado de la manera siguiente: si hay un ESCD en la vía de acceso de comunicaciones, es el número de puerto del Director de ESCON (ESCD) conectado al sistema principal. Si hay dos ESCD en la vía de acceso, es el número de puerto de la parte del sistema principal del ESCD definido con la conexión dinámica. Cuando no hay ningún ESCD en la vía de acceso de comunicaciones, este valor debe establecerse en X'01'.

dirección de red. Según ISO 7498-3, nombre que no es ambiguo en el entorno de OSI y que identifica a un conjunto de puntos de acceso a servicios de red.

dirección de subred. En comunicaciones de Internet, extensión del esquema básico de direccionamiento de IP donde una parte de la dirección de sistema principal se interpreta como dirección de red local.

dirección de todas las estaciones. En comunicaciones, sinónimo de *dirección de difusión*.

dirección de usuario de red (NUA). En comunicaciones de X.25, dirección X.121 que contiene hasta 15 dígitos en código binario.

dirección Internet. Véase *dirección IP*.

dirección IP. Dirección de 32 bits definida por Internet Protocol, norma 5, Request for Comments (RFC) 791. Normalmente, se representa mediante formato decimal con puntos.

Dirección lógica de CU. Dirección de unidad de control definida en el sistema principal para el 2216. Este valor está definido en el programa de configuración de la entrada/salida (IOCP) del sistema principal mediante la sentencia CUADD de la

instrucción de macro CNTLUNIT. La Dirección de unidad de control debe ser exclusiva para cada partición lógica definida en el mismo sistema principal.

dirección no canónica. En las LAN, formato de la transmisión de direcciones del control del acceso al medio (MAC) para adaptadores de Red en Anillo. En el formato no canónico, el bit más significativo (situado más a la izquierda) de cada byte de dirección se transmite en primer lugar. Compárese con *dirección canónica*.

directorío. Tabla de identificadores y referencias para los elementos de datos correspondientes. (I) (A)

dispositivo. Aparato mecánico, eléctrico o electrónico con un fin específico.

dominio. (1) Parte de una red de sistema en la que los recursos de proceso de datos están bajo un control común. (T) (2) En interconexión de sistemas abiertos (OSI), parte de un sistema distribuido o conjunto de objetos gestionados a los que se aplica una política común. (3) Véase *Dominio administrativo y nombre de dominio*.

Dominio administrativo. Conjunto de sistemas principales y direccionadores, y las redes de interconexión, que gestiona una sola autoridad administrativa.

dominio de direccionamiento. En comunicaciones de Internet, grupo de sistemas intermedios que utilizan un protocolo de direccionamiento para que la representación de la red en un conjunto sea la misma en cada sistema intermedio. Los dominios de direccionamiento se conectan entre sí mediante enlaces exteriores.

E

eco. En la comunicación de datos, señal de un canal de comunicaciones reflejada. Por ejemplo, en un terminal de comunicaciones, cada señal se visualiza dos veces, una cuando entra en el terminal local y otra cuando vuelve sobre el enlace de comunicaciones. Esto permite comprobar la exactitud de las señales.

EIA 232. En la comunicación de datos, especificación de la Electronic Industries Association (EIA) que define la interfaz entre el equipo terminal de datos (DTE) y el equipo de terminación de circuito de datos (DCE), que utiliza el intercambio de datos binarios serie.

Electronic Industries Association (EIA). Organización de fabricantes del campo de la electrónica que anticipa el crecimiento tecnológico de la industria, representa los puntos de vista de sus miembros y desarrolla normas para la industria.

Emulación de LAN (LE). Norma del ATM Forum que da soporte a aplicaciones de legado de LAN sobre redes ATM.

encapsulación. (1) En comunicaciones, técnica utilizada por protocolos de capa mediante la cual una capa añade a la unidad de datos de protocolo (PDU) información de control de la capa a la que da soporte. A este respecto, la capa encapsula los datos de la capa soportada. En el conjunto de protocolos de Internet, por ejemplo, un paquete contendrá información de control de la capa física, a continuación información de control de la capa de red y a continuación los datos de protocolo de la aplicación. (2) Véase también *conmutación del enlace de datos*.

enlace. Combinación de la conexión de enlace (el medio de transmisión) y dos estaciones de enlace, una a cada extremo de la conexión de enlace. Una conexión de enlace puede estar compartida entre diversos enlaces en una configuración de multipunto o Red en Anillo.

enlace lógico. Par de estaciones de enlace, una en cada uno de dos nodos adyacentes, y su conexión de enlace subyacente que proporcionan una sola conexión de capa de enlace entre los dos nodos. Pueden distinguirse diversos enlaces lógicos mientras comparten el uso del mismo medio físico de conexión de dos nodos. Ejemplos son los enlaces lógicos de 802.2 utilizados en recursos de red de área local (LAN) y los enlaces lógicos de LAP E del mismo enlace físico punto a punto entre dos nodos. El término enlace lógico también incluye los diversos canales lógicos de X.25 que comparten el uso del enlace de acceso de un DTE con una red X.25.

enlace virtual. En Open Shortest Path First (OSPF), interfaz punto a punto que conecta direccionadores de frontera separados por un área de tránsito no troncal. Puesto que los direccionadores de área forman parte del troncal OSPF, el enlace virtual conecta el troncal. Los enlaces virtuales aseguran que el troncal OSPF no se vuelva discontinuo.

equipo de terminación de circuito de datos (DCE). En una estación de datos, equipo que proporciona la conversión de señal y la codificación entre el equipo terminal de datos (DTE) y la línea. (I)

Notas:

1. El DCE puede ser un equipo independiente o parte integral del DTE o del equipo intermedio.
2. Un DCE puede realizar otras funciones que normalmente se llevan a cabo al final de red de la línea.

equipo terminal de datos (DTE). Parte de una estación de datos que funciona como origen y/o destino de datos. (I) (A)

esfera de control (SOC). Conjunto de dominios de punto de control servidos por un solo punto focal de servicios de gestión.

estación. Punto de entrada o salida de un sistema que utiliza recursos de telecomunicaciones; por ejemplo, uno o más sistemas, terminales, dispositivos y programas asociados de una ubicación determinada que pueden enviar o recibir datos sobre una línea de telecomunicaciones.

estación de configuración Nways Switch. Estación de OS/2 dedicada que ejecuta una versión autónoma de la herramienta Nways Switch Configuration Tool (NCT). Se utiliza para generar una base de datos de configuración de red y debe instalarse como consola remota.

estación de enlace. (1) Componentes de hardware y software de un nodo que representan una conexión con un nodo adyacente sobre un enlace específico. Por ejemplo, si el nodo A es el extremo primario de una línea multipunto que se conecta con tres nodos adyacentes, el nodo A tendrá tres estaciones de enlace que representarán las conexiones con los nodos adyacentes. (2) Véase también *estación de enlace adyacente (ALS)*.

estación de gestión. En comunicaciones de Internet, sistema responsable de la gestión de toda una red o de parte de la misma. La estación de gestión se comunica con agentes de gestión de red que residen en el nodo gestionado por medio de un protocolo de gestión de red, como, por ejemplo, Simple Network Management Protocol (SNMP).

estación de gestión de red. En el protocolo Simple Network Management Protocol (SNMP), estación que ejecuta programas de aplicación de gestión que supervisan y controlan elementos de red.

estación de soporte de red. Procesador utilizado para realizar operaciones en Nways Switch y darle servicio técnico localmente. Lo utilizan el administrador o el personal de servicio encargados de Nways Switch.

estado de los enlaces. En los protocolos de direccionamiento, información anunciada sobre las interfaces utilizables y los direccionadores contiguos a un direccionador o una red asequibles. La base de datos topológica del protocolo se forma a partir de los anuncios reunidos sobre el estado de los enlaces.

estructura de la información de gestión (SMI). (1) En el protocolo Simple Network Management Protocol (SNMP), normas utilizadas para definir los objetos a los que puede accederse por medio de un protocolo de gestión de red. (2) En OSI, conjunto de normas relativas a la información de gestión. El conjunto incluye el *Management Information Model* y las *Guidelines for the Definition of Managed Objects*.

Ethernet. Red de área local de banda base de 10 Mbps que permite que diversas estaciones accedan al medio de transmisión a voluntad sin coordinación previa, evita la contención utilizando la detección y deferencia de portadora y resuelve la contención utilizando la detección de colisión y la retransmisión retardada. Ethernet utiliza el acceso múltiple con detección de portadora y detección de colisión (CSMA/CD).

excepción. Condición anormal, como, por ejemplo, un error de E/S encontrado durante el proceso de un conjunto de datos o archivo.

extensión de ruta (REX). En SNA, componentes de red de control de la vía de acceso, incluido un enlace periférico, que componen la parte de una vía de acceso que está entre un nodo de subárea y una unidad de red dirigible (NAU) de un nodo periférico adyacente. Véase también *ruta explícita (ER)*, *vía de acceso y ruta virtual (VR)*.

Exterior Gateway Protocol (EGP). En el conjunto de protocolos de Internet, protocolo utilizado entre dominios y sistemas autónomos que permite anunciar e intercambiar información sobre la asequibilidad de la red. Las direcciones de red IP de un sistema autónomo se anuncian en otro sistema autónomo por medio de direccionadores que participan de EGP. Un ejemplo de EGP es Border Gateway Protocol (BGP). Compárese con Interior Gateway Protocol (IGP).

F

fax. Copia impresa que se recibe de una máquina de facsímil. Sinónimo con *telecopia*.

File Transfer Protocol (FTP). En el conjunto de protocolos de Internet, protocolo de capa de aplicación que utiliza servicios de TCP y Telnet para transferir archivos de datos generales entre máquinas o sistemas principales.

fluctuación. (1) Variaciones no acumulativas a corto plazo de los instantes significativos de una señal digital respecto a sus posiciones ideales en el tiempo. (2) Variaciones no deseadas de una señal digital transmitida. (3) Variaciones en el retardo de la red.

formato decimal con puntos. Representación sintáctica de un entero de 32 bits que consta de cuatro números de 8 bits escritos en base 10 con puntos que los separan. Se utiliza para representar direcciones IP.

fragmentación. (1) Proceso consistente en dividir un datagrama en partes más pequeñas, o fragmentos, para que se ajuste a las posibilidades del medio físico por el que se va a transmitir. (2) Véase también *segmentación*.

fragmento. Véase *fragmentación*.

Frame Relay. (1) Norma de interfaz que describe el límite entre el equipo de un usuario y una red de paquetes rápidos. En los sistemas Frame-Relay, se eliminan las tramas defectuosas; la recuperación se produce de extremo a extremo en lugar de efectuarse salto a salto. (2) Técnica derivada de la norma de canal D de red digital de servicios integrados (RDSI). Supone que las conexiones son fiables y prescinde de la actividad general de control y detección de errores en la red.

funcionamiento en modalidad de paquete. Sinónimo de *conmutación de paquetes*.

función de puente. En las LAN, el reenvío de una trama de un segmento de LAN a otro. El destino está especificado mediante la dirección de subcapa del control del acceso al medio (MAC) codificada en el campo de dirección de destino de la cabecera de la trama.

función de puente de ruta de origen. En las LAN, método de función de puente que utiliza el campo de información de direccionamiento de la cabecera del control del acceso al medio (MAC) de IEEE 802.5 de una trama para determinar los anillos o segmentos de Red en Anillo que debe recorrer la trama. El nodo de origen inserta el campo de información de direccionamiento en la cabecera del MAC. La información del campo de información de direccionamiento deriva de los paquetes exploradores generados por el sistema principal de origen.

función de puente local. Función de un programa de puente que permite que un solo puente conecte diversos segmentos de LAN sin la utilización de un enlace de telecomunicaciones. Compárese con *función de puente remota*.

función de puente remota. Función de un puente que permite que dos puentes conecten diversas LAN utilizando un enlace de telecomunicaciones. Compárese con *función de puente local*.

función de puente transparente. En las LAN, método para relacionar redes de área local individuales entre sí en el nivel del control del acceso al medio (MAC). Un puente transparente almacena las tablas que contienen direcciones del MAC para que las tramas que ve el puente puedan reenviarse a otra LAN si las tablas lo indican así.

función de túnel. Trata a una red de transporte como si fuera una sola LAN o un solo enlace de comunicaciones. Véase también *encapsulación*.

G

gestión de red. Proceso consistente en planificar, organizar y controlar un proceso de datos o sistema de información orientado a las comunicaciones.

gestor de red. Programa o grupo de programas que se utiliza para supervisar y gestionar una red así como para diagnosticar los problemas de la misma.

grupo de transmisión (TG). (1) Conexión entre nodos adyacentes que se identifica mediante un número de grupo de transmisión. (2) En una red de subárea, enlace o grupo de enlaces entre nodos adyacentes. Cuando un grupo de transmisión está compuesto por un grupo de enlaces, los enlaces se ven como un solo enlace lógico y el grupo de transmisión se denomina *grupo de transmisión multienlace (MLTG)*. Un *grupo de transmisión multienlace de mezcla de medios (MMMLTG)* contiene enlaces de diferentes tipos de medios (por ejemplo, Red en Anillo, SDLC conmutado, SDLC no conmutado y enlaces Frame-Relay). (3) En una red APPN, enlace entre nodos adyacentes. (4) Véase también *grupos de transmisión paralelo*.

grupos de transmisión paralelo. Diversos grupos de transmisión entre nodos adyacentes, teniendo cada grupo un número de grupo de transmisión distinto.

H

Hello. Protocolo utilizado por un grupo de direccionadores que cooperan y se apoyan entre sí para poder descubrir rutas de retardo mínimo.

heurístico. Perteneciente a métodos exploratorios para la resolución de problemas en los que se descubren soluciones mediante una evaluación del progreso realizada respecto al resultado final.

histéresis. Cantidad que indica cuánto debe cambiar la temperatura una vez pasado el umbral del establecimiento de alerta y antes de que se elimine la condición de alerta.

horizonte dividido. Técnica destinada a minimizar el tiempo para conseguir la convergencia en la red. Un direccionador registra la interfaz sobre la que ha recibido una ruta en particular y no propaga su información sobre la ruta otra vez sobre la misma interfaz.

I

identificación de intercambio (XID). Tipo específico de unidad básica de enlace que se utiliza para la comunicación de características de nodo y enlace entre nodos adyacentes. Los XID se intercambian entre estaciones de enlace antes de la activación del enlace y durante la misma para establecer y negociar las características de enlace y nodo, y después de la activación del enlace para comunicar los cambios de estas características.

identificador de conexión de enlace de datos (DLCI). Identificador numérico de un subpuerto Frame-Relay o segmento de PVC en una red

Frame-Relay. Cada subpuerto de un puerto Frame-Relay individual tiene un DLCI exclusivo. La tabla siguiente, extraída de la norma T1.618 del American National Standards Institute (ANSI) y la norma Q.922 de la Comisión Consultiva de la telefonía y telegrafía internacionales (ITU-T/CCITT), indica las funciones asociadas con determinados valores de DLCI:

Valores de DLCI	Función
0	Señalización de canal de entrada
1–15	Se reserva
16–991	Se asigna utilizando procedimientos de conexión de Frame-Relay
992–1007	Gestión de capa 2 de servicio de portador de Frame-Relay
1008–1022	Se reserva
1023	Gestión de capa de canal de entrada

identificador de puente. Campo de 8 bytes que se utiliza en un protocolo de árbol de expansión y está compuesto por la dirección MAC del puerto con el identificador de puerto más bajo y un valor definido por el usuario.

identificador de red. (1) En TCP/IP, parte de la dirección IP que define a una red. La longitud del identificador de red depende del tipo de la clase de red (A, B o C). (2) Nombre de 1 a 8 bytes seleccionado por el cliente o nombre registrado por IBM que identifica de manera exclusiva una subred específica.

inhabilitado. (1) Perteneciente a un estado de una unidad de proceso que evita la aparición de determinados tipos de interrupciones. (2) Perteneciente al estado en el cual una unidad de control de transmisión o unidad de respuestas audibles no puede aceptar llamadas de entrada de una línea.

inhabilitar. Convertir en no funcional.

Integrated Digital Network Exchange (IDNX).

Procesador que integra aplicaciones a base de voz, datos e imágenes. También gestiona los recursos de transmisión y se conecta a multiplexores y sistemas de soporte de gestión de redes. Permite la integración de equipos de diferentes proveedores.

intercambio de conmutaciones de datos (DSE).

Equipo instalado en una ubicación individual para proporcionar funciones de conmutación, como, por ejemplo, conmutación del circuito, conmutación de mensajes y conmutación de paquetes. (I)

interconexión de sistemas abiertos (OSI).

(1) Interconexión de sistemas abiertos que sigue las normas de la organización internacional para la normalización (ISO) para el intercambio de información. (T) (A) (2) Utilización de

procedimientos normalizados para permitir la interconexión de sistemas de proceso de datos.

Nota: La arquitectura OSI establece una infraestructura para coordinar el desarrollo de normas actuales y futuras de cara a la interconexión de sistemas. Las funciones de red se dividen en siete capas. Cada capa representa un grupo de funciones relacionadas de proceso de datos y comunicación que pueden llevarse a cabo de una manera estándar para dar soporte a diferentes aplicaciones.

interfaz. (1) Límite compartido entre dos unidades funcionales en cuya definición entran características funcionales, características de señalización u otras características según lo que corresponda. El concepto incluye la especificación de la conexión de dos dispositivos que tienen funciones diferentes. (T) (2) Hardware y/o software para el enlace de sistemas, programas o dispositivos.

interfaz de gestión local (LMI). Véase *protocolo de interfaz de gestión local (LMI)*.

interfaz de unidad de conexión (AUI). En una red de área local, interfaz entre la unidad de conexión al medio y el equipo terminal de datos de una estación de datos. (I) (A)

Interior Gateway Protocol (IGP). En el conjunto de protocolos de Internet, protocolo utilizado para propagar información sobre la asequibilidad y direccionamiento de la red dentro de un sistema autónomo. Ejemplos de IGP son Routing Information Protocol (RIP) y Open Shortest Path First (OSPF).

internet. Conjunto de redes interconectadas por una serie de direccionadores que les permiten funcionar como una sola red grande. Véase también *Internet*.

Internet. Red internet administrada por la Internet Architecture Board (IAB) y compuesta por grandes redes troncales nacionales así como por muchas redes regionales y de campus en todo el mundo. Internet utiliza el conjunto de protocolos de Internet.

Internet Architecture Board (IAB). Corporación técnica que supervisa el desarrollo del conjunto de protocolos de Internet conocidos como TCP/IP.

Internet Control Message Protocol (ICMP). Protocolo utilizado para manejar mensajes de control y errores en la capa de Internet Protocol (IP). Los informes sobre problemas y destinos incorrectos de datagramas se devuelven al origen del datagrama. ICMP forma parte de Internet Protocol.

Internet Control Protocol (ICP). Protocolo de Virtual NEtworking System (VINES) que proporciona notificaciones de excepciones, notificaciones sobre métrica y el soporte del programa PING. Véase también *RouTing update Protocol (RTP)*.

Internet Engineering Task Force (IETF). Grupo de operaciones de la Internet Architecture Board (IAB) que es responsable de la resolución de las necesidades técnicas de la Internet a corto plazo.

Internet Protocol (IP). Protocolo sin conexiones que direcciona datos a través de una red o redes interconectadas. IP actúa como intermediario entre las capas de protocolos superiores y la red física. No obstante, este protocolo no proporciona recuperación de errores ni control del flujo ni garantiza la fiabilidad de la red física.

Internetwork Packet Exchange (IPX). (1) Protocolo de red utilizado para conectar servidores Novell, o cualquier estación de trabajo o direccionador que implemente IPX, con otras estaciones de trabajo. Aunque es similar a Internet Protocol (IP), IPX utiliza unos formatos de paquete y una terminología diferentes. (2) Véase también *Xerox Network Systems (XNS)*.

interoperatividad. Posibilidad de comunicarse, ejecutar programas o transferir datos entre diversas unidades funcionales de tal forma que el usuario necesite tener poco conocimiento, o ninguno, de las características exclusivas de estas unidades. (T)

interposición. (1) Alternar dos o más operaciones o funciones en el uso solapado de un recurso del sistema. (2) En transmisión de datos, alternar paquetes de una corriente de datos con paquetes de otra.

Inverse Address Resolution Protocol (InARP). En el conjunto de protocolos de Internet, protocolo utilizado para ubicar una dirección de protocolo mediante la dirección de hardware conocida. En un contexto de Frame-Relay, identificador de conexión de enlace de datos (DLCI) es sinónimo de dirección de hardware conocida.

IPPN. Interfaz que otros protocolos pueden utilizar para transportar datos sobre IP.

IPXWAN. Protocolo de Novell que se utiliza para intercambiar información de direccionador a direccionador antes de intercambiar información de direccionamiento de Internetwork Packet Exchange (IPX) estándar y tráfico sobre redes de área amplia (WAN).

L

LAN Network Manager (LNM). Programa bajo licencia de IBM que permite que un usuario gestione y supervise los recursos de la LAN desde una estación de trabajo central.

LE. Emulación de LAN. Norma del ATM Forum que da soporte a aplicaciones del tipo LAN sobre redes ATM.

LEC. Cliente de emulación de LAN. Componente de LAN Emulation Service que representa a los usuarios de la LAN emulada.

LECS. Servidor de configuración de emulación de LAN. Componente de LAN Emulation Service que centraliza y difunde datos de configuración.

LES. Servidor de emulación de LAN. Componente de LAN Emulation Service que resuelve destinos de LAN en direcciones ATM.

línea tronco. Línea de gran velocidad que conecta dos Nways Switch. Puede ser un cable coaxial, un cable de fibra u ondas de radio, por ejemplo, y puede alquilarse en empresas de telecomunicación.

local. (1) Perteneciente a un dispositivo al que se accede directamente sin utilizar una línea de telecomunicaciones. (2) Compárese con *remoto*. (3) Sinónimo de *conectado mediante canal*.

LP. partición lógica

LPAR. lógicamente particionada

M

mandato ping. Mandato que envía un paquete de petición con eco de Internet Control Message Protocol (ICMP) a una pasarela, direccionador o sistema principal esperando recibir una respuesta.

máscara. (1) Patrón de caracteres utilizado para controlar la retención o eliminación de partes de otro patrón de caracteres. (I) (A) (2) Utilizar un patrón de caracteres para controlar la retención o eliminación de partes de otro patrón de caracteres. (I) (A)

máscara de dirección. Respecto a las subredes de internet, máscara de 32 bits utilizada para identificar los bits de dirección de subred de la parte del sistema principal de una dirección IP. Sinónimo con *máscara de subred* y *máscara de subred (grupo de nodos)*.

máscara de subred. Sinónimo de *máscara de dirección*.

máscara de subred (grupo de nodos). Sinónimo de *máscara de dirección*.

memoria de almacenamiento dinámico. Cantidad de RAM utilizada para asignar estructuras de datos dinámicamente.

memoria de sólo lectura (ROM). Memoria en la que el usuario no puede modificar los datos almacenados salvo en condiciones especiales.

memoria instantánea. Dispositivo de almacenamiento de datos que puede programarse y borrarse y que no necesita alimentación continua. La ventaja principal de la memoria instantánea sobre otros dispositivos de

almacenamiento de datos que pueden programarse y borrarse es que puede volver a programarse sin quitarla de la placa de circuitos.

mensaje hello. (1) Mensaje enviado periódicamente para establecer y probar la asequibilidad entre direccionadores o entre direccionadores y sistemas principales. (2) En el conjunto de protocolos de Internet, mensaje definido por el protocolo Hello como Interior Gateway Protocol (IGP).

métrica. En comunicaciones de Internet, valor asociado con una ruta que se utiliza para establecer diferencias entre los múltiples puntos de entrada o salida respecto al mismo sistema autónomo. Se prefiere la ruta con la métrica inferior.

MIB. (1) Módulo de la MIB. (2) Base de la información de gestión.

MIB estándar. En el protocolo Simple Network Management Protocol (SNMP), módulo de la MIB que se ubica bajo la rama de gestión de la estructura de la información de gestión (SMI) y que se considera una norma en Internet Engineering Task Force (IETF).

MILNET. Red militar que formaba parte de ARPANET en un principio. Quedó separada de ARPANET en 1984. MILNET proporciona un servicio de red fiable para las instalaciones militares.

modalidad lógicamente particionada (LPAR). Función de algunos procesadores principales en que el proceso se divide en particiones lógicas (LP) para parecer diversos procesadores. En modalidad LPAR, el adaptador de ESCON puede compartir una conexión de fibra física con diversas particiones de sistema principal.

modalidad LPAR. Modalidad lógicamente particionada (LPAR).

modelo de referencia interconexión de sistemas abiertos (OSI). Modelo que describe los principios generales de interconexión de sistemas abiertos así como la finalidad y la ordenación jerárquica de sus siete capas. (T)

módem (modulador/demodulador). (1) Unidad funcional que modula y demodula señales. Una de las funciones de un módem es permitir que los datos digitales se transmitan sobre recursos de transmisión analógicos. (T) (A) (2) Dispositivo que convierte los datos digitales de un sistema en una señal analógica que pueda transmitirse en una línea de telecomunicaciones, y convierte la señal analógica recibida en datos para el sistema.

modulación en código de pulsaciones (PCM). Norma adoptada para la digitalización de una señal de voz analógica. En la PCM, se realiza un muestreo de la voz a una velocidad de ocho kHz y cada muestra se codifica en una trama de 8 bits.

módulo. (1) Perteneciente a un módulo matemático; por ejemplo, 9 equivale a 4 módulo 5. (2) Véase también *módulo (diferencia)*.

módulo. En Nways Switch, unidad de hardware funcional empaquetada que contiene tarjetas lógicas, conectores y luces. Los módulos se utilizan para empaquetar adaptadores, acopladores de interfaz de línea, extensiones de servidor de voz y otros componentes. Todos los módulos pueden **conectarse en caliente** en los subbastidores lógicos.

módulo (diferencia). Número, como por ejemplo un entero positivo, de una relación que divide la diferencia entre dos números relacionados sin dejar un resto; por ejemplo, 9 y 4 tienen un módulo de 5 ($9 - 4 = 5$; $4 - 9 = -5$; y 5 divide tanto 5 como -5 sin dejar un resto).

multidifusión. (1) Transmisión de los mismos datos a un grupo seleccionado de destinos. (T) (2) Forma especial de difusión en que se entregan copias de un paquete a un subconjunto de todos los destinos posibles solamente.

multiplexación de la división del tiempo (TDM). Véase *canalización*.

N

Name Binding Protocol (NBP). En redes AppleTalk, protocolo que proporciona la función de conversión de nombre a partir del nombre (serie de caracteres) de una entidad (recurso) AppleTalk en una dirección IP AppleTalk (número de 16 bits) en la capa de transporte.

NetBIOS. Network Basic Input/Output System. Interfaz estándar para redes, IBM PC (Personal Computer) y PC compatibles, que se utiliza en las LAN para proporcionar funciones de mensajes, de servidor de impresión y de servidor de archivos. Los programas de aplicación que utilizan NetBIOS no necesitan manejar los detalles de protocolos de control de enlace de datos (DLC) de la LAN.

nivel de enlace. (1) Parte de la recomendación X.25 que define el protocolo de enlace utilizado para entrar datos en la red y sacarlos de la misma a través del enlace dúplex que conecta la máquina del abonado con el nodo de red. LAP y LAPB son los protocolos de acceso de enlace recomendados por la CCITT. (2) Véase *nivel de enlace de datos*.

nivel de enlace de datos. (1) En la estructura jerárquica de una estación de datos, nivel conceptual de control o lógica de proceso entre la lógica de alto nivel y el enlace de datos que mantiene el control del enlace de datos. El nivel de enlace de datos realiza funciones tales como la inserción de bits de transmisión y supresión de bits de recepción; interpretación de campos de dirección y control; generación, transmisión e interpretación de mandatos y respuestas; y cálculo e interpretación de secuencias de comprobación de

trama. Véase también *nivel de paquete* y *nivel físico*. (2) En comunicaciones de X.25, sinónimo de *nivel de trama*.

nivel de trama. Sinónimo con *nivel de enlace de datos*. Véase *nivel de enlace*.

nodo. (1) En una red, punto donde una o más unidades funcionales conectan canales o circuitos de datos. (I) (2) Cualquier dispositivo conectado a una red que transmite y recibe datos.

nodo Advanced Peer-to-Peer Networking (APPN). Nodo de red APPN o nodo final APPN.

nodo de destino. Nodo al que se envían datos o una petición.

nodo de esfera de control (SOC). Nodo que está incluido directamente en la esfera de control de un punto focal. Un nodo de SOC ha intercambiado elementos de habilitación de los servicios de gestión con su punto focal. Un nodo final APPN puede ser un nodo de SOC si da soporte a la función de intercambio de elementos de habilitación de los servicios de gestión.

nodo de red Advanced Peer-to-Peer Networking (APPN). Nodo que ofrece un amplio rango de servicios de usuario final y que puede proporcionar lo siguiente:

- servicios de directorios distribuidos, incluido el registro de los recursos del dominio con un servidor de directorios central
- Intercambios de bases de datos de topología con otros nodos de red APPN, lo que permite que los nodos de red de la red seleccionen las rutas óptimas para sesiones de LU-LU basándose en las clases de servicio solicitadas
- Servicios de sesiones para los nodos finales clientes y las LU locales
- Servicios de direccionamiento intermedio de una red APPN

nodo de red APPN. Véase *nodo de red Advanced Peer-to-Peer Networking (APPN)*.

nodo de red de entrada baja (LEN). Nodo que proporciona un rango de servicios de usuario final, se conecta directamente con otros nodos utilizando protocolos de igual a igual y hace derivar servicios de red de un nodo de red APPN adyacente implícitamente, es decir, sin el uso directo de sesiones de CP-CP.

nodo de red (NN). Véase *nodo de red Advanced Peer-to-Peer Networking (APPN)*.

nodo final Advanced Peer-to-Peer Networking (APPN). Nodo que proporciona un amplio rango de servicios de usuario final y da soporte a las sesiones entre su punto de control (CP) local y el CP de un nodo de red adyacente. Utiliza estas sesiones con el fin de

registrar dinámicamente sus recursos con el CP adyacente (su servidor de nodos de red) para enviar y recibir peticiones de búsqueda en directorios y obtener servicios de gestión. Un nodo final APPN también puede conectarse a una red de subárea como nodo periférico o a otros nodos finales.

nodo final de red de entrada baja (LEN). Nodo LEN que recibe servicios de red de un nodo de red APPN adyacente.

nodo final (EN). (1) Véase *nodo final Advanced Peer-to-Peer Networking (APPN)* y *nodo final de red de entrada baja (LEN)*. (2) En comunicaciones, nodo que se conecta frecuentemente a un solo enlace de datos y no puede realizar funciones de direccionamiento intermedio.

nodo intermedio. Nodo que está al final de más de una rama. (T)

nodos adyacentes. Dos nodos conectados conjuntamente por una vía de acceso, como mínimo, que no conecta ningún otro nodo. (T)

nombre de comunidad. En el protocolo Simple Network Management Protocol (SNMP), serie de octetos que identifica a una comunidad.

nombre de dominio. En el conjunto de protocolos de Internet, nombre de un sistema principal. Un nombre de dominio está compuesto por una secuencia de subnombres separados por un carácter delimitador. Por ejemplo, si el nombre de dominio calificado al completo (FQDN) de un sistema principal es

ra1vm7.vnet.ibm.com, cada uno de los siguientes es un nombre de dominio:

- ra1vm7.vnet.ibm.com
- vnet.ibm.com
- ibm.com

notación de sintaxis de abstracción 1 (ASN.1). Método de Interconexión de Sistemas Abiertos (OSI) para la sintaxis de abstracción que se especifica en las normas siguientes:

- ITU-T recomendación X.208 (1988) | ISO/IEC 8824: 1990
- ITU-T recomendación X.680 (1994) | ISO/IEC 8824-1: 1994

Véase también *normas básicas de codificación (BER)*.

número de LP. Número de partición lógica. Permite que diversas particiones lógicas de sistema principal, LP, compartan una sola fibra de ESCON. Este valor está definido en el programa de configuración de la entrada/salida (IOCP) del sistema principal mediante la instrucción de macro RESOURCE. Si el sistema principal no utiliza EMIF, utilice el valor por omisión de 0 para el número de LP.

número de puerto. En comunicaciones de Internet, identificación de una entidad de aplicación para el servicio de transporte.

número de secuencia. En comunicaciones, número asignado a una trama o paquete en particular para controlar el flujo de la transmisión y la recepción de datos.

número de sistema autónomo. En TCP/IP, número asignado a un sistema autónomo por la misma autorización central que también asigna direcciones IP. El número de sistema autónomo hace posible que los algoritmos de direccionamiento automatizado distingan los sistemas autónomos.

Nways Switch. Sinónimo con IBM 2220 Nways BroadBand Switch.

O

objeto de la MIB. Sinónimo de *variable de la MIB*.

Open Shortest Path First (OSPF). En el conjunto de protocolos de Internet, función que proporciona transferencia de información intradominio. Como alternativa al protocolo Routing Information Protocol (RIP), OSPF permite el direccionamiento de menor coste y lo maneja en grandes redes regionales o corporativas.

organización internacional para la normalización (ISO). Organización de corporaciones nacionales de normas de varios países establecida para promocionar el desarrollo de normas con el fin de facilitar el intercambio internacional de artículos y servicios además de desarrollar la cooperación en la actividad intelectual, científica, tecnológica y económica.

origen. Unidad lógica (LU) externa o programa de aplicación de donde parten un mensaje u otros datos. Véase también *destino*.

P

paquete. En la comunicación de datos, secuencia de dígitos binarios, con inclusión de señales de control y datos, que se transmite y se conmuta como un todo compuesto. Los datos, las señales de control y, posiblemente, la información de control de errores se ordenan siguiendo un formato específico. (I)

paquete de datos. En comunicaciones de X.25, paquete utilizado para la transmisión de datos de usuario dentro de un circuito virtual en la interfaz DTE/DCE.

paquete de petición de llamada. (1) Paquete de supervisión de llamada que un equipo terminal de datos (DTE) transmite con el fin de solicitar que se establezca una conexión para una llamada en la red. (2) En

comunicaciones de X.25, paquete de supervisión de llamada transmitido por un DTE para solicitar el establecimiento de una llamada en la red.

paquete de petición de restablecimiento. En comunicaciones X.25, paquete transmitido por el equipo terminal de datos (DTE) al equipo de terminación de circuito de datos (DCE) para solicitar que se restablezca una llamada virtual o un circuito virtual permanente. En el paquete también puede especificarse la razón de la petición.

paquete de recepción no preparada (RNR). Véase *paquete de RNR*.

paquete de RNR. Paquete utilizado por un equipo terminal de datos (DTE) o por un equipo de terminación de circuito de datos (DCE) con el fin de indicar una incapacidad temporal para aceptar paquetes adicionales de petición de llamada virtual o circuito virtual permanente.

paquete explorador. En las LAN, paquete que está generado por el sistema principal de origen y que atraviesa toda la parte de direccionamiento de origen de una LAN con el fin de recoger información sobre las posibles vías de acceso que se encuentran disponibles para el sistema principal.

parámetro de configuración. Variable de una definición de configuración cuyos valores pueden caracterizar la relación de un producto con otros productos de la misma red o pueden definir características del producto en sí.

par de valores de atributo (AVP). Método uniforme de codificación de tipos y cuerpos de mensajes. Este método maximiza la extensibilidad mientras permite la interoperatividad de L2TP.

partición lógica. Número asignado a una partición de un sistema principal que puede funcionar en modalidad lógicamente particionada (LPAR). En modalidad LPAR, el adaptador de ESCON puede compartir una conexión de fibra física con diversas particiones de sistema principal.

pasarela. (1) Unidad funcional que interconecta dos redes de sistema con arquitecturas de red diferentes. Una pasarela conecta redes o sistemas de arquitecturas diferentes. Un puente interconecta redes o sistemas con la misma arquitectura o con arquitecturas similares. (T) (2) En la Red en Anillo de IBM, dispositivo y software asociado al mismo que conectan una red de área local a otra red de área local o a un sistema principal que utiliza protocolos de enlace lógico diferentes. (3) En TCP/IP, sinónimo de *direccionador*.

pasarela exterior. En comunicaciones de Internet, pasarela de un sistema autónomo que comunica con otro sistema autónomo. Compárese con *pasarela interior*.

pasarela interior. En comunicaciones de Internet, pasarela que sólo comunica con su propio sistema autónomo. Compárese con *pasarela exterior*.

período de duración (TTL). Técnica utilizada por los protocolos de entrega de mayor eficacia para impedir que los paquetes se repitan en bucle de manera interminable. El paquete se elimina si el contador de TTL alcanza el valor de 0.

petionario de LU dependientes (DLUR). Nodo final APPN o nodo de red APPN que posee LU dependientes pero solicita que un servidor de LU dependientes proporcione los servicios del SSCP para estas LU dependientes.

Point-to-Point Protocol (PPP). Protocolo que proporciona un método para encapsular y transmitir paquetes sobre enlaces serie punto a punto.

portadora. Tren de pulsaciones u ondas eléctricas o electromagnéticas que puede variar según una señal con información a transmitir sobre un sistema de comunicaciones. (T)

procesador de componente frontal. Procesador, como, por ejemplo, el IBM 3745 ó el 3174, que releva a un sistema principal de las tareas de control de comunicaciones.

proceso a tiempo real. Manipulación de los datos que un proceso necesita o genera mientras el proceso está en funcionamiento. Normalmente, los resultados se utilizan para influir en el proceso y quizá en procesos relacionados, mientras se está desarrollando.

proporción de pérdida de un paquete. Probabilidad que tiene un paquete de no alcanzar su destino o de no alcanzarlo dentro del período especificado.

protocolo. (1) Conjunto de normas semánticas y sintácticas que determinan el comportamiento de las unidades funcionales a la hora de conseguir la comunicación. (I) (2) En la arquitectura interconexión de sistemas abiertos, conjunto de normas semánticas y sintácticas que determinan el comportamiento de las entidades de la misma capa a la hora de desempeñar funciones de comunicación. (T) (3) En SNA, significados y normas de puesta en secuencia de las peticiones y respuestas que se utilizan para gestionar la red, transferir datos y sincronizar los estados de los componentes de la red. Sinónimo con *disciplina de control de línea y disciplina de línea*. Véase *protocolo delimitador y protocolo de enlace*.

protocolo de acceso de enlace equilibrado (LAPB). Protocolo utilizado para acceder a una red X.25 en el nivel de enlace. LAPB es un protocolo simétrico, asíncrono y dúplex que se utiliza en la comunicación punto a punto.

protocolo de control de enlace lógico (LLC). En una red de área local, protocolo que dirige el

intercambio de tramas de transmisión entre estaciones de datos independientemente de cómo está compartido el medio de transmisión. (T) El protocolo de LLC se desarrolló en la comisión de IEEE 802 y es común a todas las normas de LAN.

protocolo de control del acceso al medio (MAC).

En una red de área local, protocolo que dirige el acceso al medio de transmisión, teniendo en cuenta los aspectos topológicos de la red, con el fin de permitir el intercambio de datos entre estaciones de datos. (T)

protocolo de direccionamiento. Técnica utilizada por un direccionador para encontrar otros direccionadores y mantener información actualizada sobre la mejor manera de acceder a las redes asequibles.

protocolo de interfaz de gestión local (LMI). En un NCP, conjunto de procedimientos y mensajes de gestión de red Frame-Relay utilizados por nodos Frame-Relay adyacentes para intercambiar información de estado de línea sobre el DLCI X'00'. Un NCP da soporte tanto a la versión del protocolo de LMI del American National Standards Institute (ANSI) como a la de la Comisión Consultiva de la Telefonía y Telegrafía Internacionales (ITU-T/CCITT). Estas normas se refieren al protocolo de LMI como *pruebas de verificación de integridad de enlace (LIVT)*.

prueba de bucle de retorno. Prueba donde las señales de un comprobador se repiten en bucle en un módem u otro elemento de red hacia el comprobador para tomar medidas que determinen o verifiquen la calidad de la vía de acceso de comunicaciones.

puente. Unidad funcional que interconecta diversas LAN (local o remotamente) que utilizan el mismo protocolo de control de enlace lógico pero que pueden utilizar diferentes protocolos de control del acceso al medio. Un puente reenvía una trama a otro puente basándose en la dirección del control del acceso al medio (MAC).

puente de ruta. Función de un programa de puente de IBM que permite que dos sistemas de puente utilicen un enlace de telecomunicaciones para conectar dos LAN. Cada sistema de puente se conecta directamente a una de las LAN y el enlace de telecomunicaciones conecta los dos sistemas de puente.

puente raíz. Puente que es la raíz de un árbol de expansión formado entre otros puentes activos de la red de funciones de puente. El puente raíz origina y transmite unidades de datos de protocolo de puente (BPDU) a otros puentes activos para mantener la topología de árbol de expansión. Es el puente con la prioridad superior de la red.

puentes paralelo. Par de puentes conectados al mismo segmento de LAN que crean vías de acceso redundantes para el segmento.

puerto. (1) Punto de acceso para la entrada o salida de datos. (2) Conector de un dispositivo al que se conectan cables para otros dispositivos, como, por ejemplo, estaciones de pantalla o impresoras. (3) Representación de una conexión física con el hardware de enlace. A veces, un puerto viene referido como adaptador; no obstante, en un adaptador puede haber más de un puerto. Un solo proceso de DLC puede controlar uno o más puertos. (4) En el conjunto de protocolos de Internet, número de 16 bits utilizado para la comunicación entre TCP o el protocolo User Datagram Protocol (UDP) y una aplicación o protocolo de nivel superior. Algunos protocolos, como, por ejemplo, File Transfer Protocol (FTP) y Simple Mail Transfer Protocol (SMTP), utilizan el mismo número de puerto conocido en todas las implementaciones de TCP/IP. (5) Abstracción utilizada por protocolos de transporte para establecer diferencias entre los diversos destinos en una máquina de sistema principal. (6) Sinónimo con *socket*.

puerto de destino. Adaptador asíncrono de 8 puertos que sirve de punto de conexión con un servicio serie.

punto de acceso a servicios de destino (DSAP). En SNA y TCP/IP, dirección lógica que permite que un sistema direcciona datos desde un dispositivo remoto al soporte de comunicaciones correspondiente. Compárese con *punto de acceso a servicios de origen (SSAP)*.

punto de acceso a servicios de origen (SSAP). En SNA y TCP/IP, dirección lógica que permite que un sistema envíe datos a un dispositivo remoto desde el soporte de comunicaciones correspondiente. Compárese con *punto de acceso a servicios de destino (DSAP)*.

punto de acceso a servicios (SAP). (1) En la arquitectura interconexión de sistemas abiertos (OSI), punto en el que una entidad de una capa proporciona los servicios de esta capa a una entidad de la capa superior más próxima. (T) (2) Punto lógico que queda disponible mediante un adaptador y donde puede recibirse y transmitirse información. Muchos enlaces pueden terminar en un solo punto de acceso a servicios.

punto de control (CP). (1) Componente de un nodo APPN o LEN que gestiona los recursos de dicho nodo. En un nodo APPN, el CP puede dedicarse a establecer sesiones de CP-CP con otros nodos APPN. En un nodo de red APPN, el CP también proporciona servicios a nodos finales adyacentes de la red APPN. (2) Componente de un nodo que gestiona los recursos de dicho nodo y, opcionalmente, proporciona servicios a otros nodos de la red. Pueden citarse como ejemplos el punto de control de servicios del sistema (SSCP) de un nodo de subárea de tipo 5, el punto de control de nodo de red (NNCP) de un nodo de red APPN y el punto de

control de nodo final (ENCP) de un nodo final APPN o LEN. Un SSCP y un NNCP pueden proporcionar servicios a otros nodos.

punto de control de servicios del sistema (SSCP).

Componente de una red de subárea destinado a gestionar la configuración, coordinar las peticiones del operador de red y las de determinación de problemas y proporcionar servicios de directorios además de otros servicios de sesiones para los usuarios de la red. Diversos SSCP, cooperando como iguales entre sí, pueden dividir la red en dominios de control y tener, cada uno de los SSCP, una relación de control jerárquica con las unidades físicas y las unidades lógicas de su propio dominio.

punto de entrada (EP). En SNA, nodo de tipo 2.0, tipo 2.1, tipo 4 ó tipo 5 que proporciona soporte de gestión de redes distribuidas. Envía datos de gestión de redes sobre sí mismo y los recursos que controla a un punto focal para el proceso centralizado, y recibe y ejecuta los mandatos iniciados por el punto focal para gestionar y controlar sus recursos.

R

rastreo. (1) Registro de la ejecución de un programa de sistema. Muestra las secuencias en que se han ejecutado las instrucciones. (A) (2) Para los enlaces de datos, registro de las tramas y bytes transmitidos o recibidos.

recepción no preparada (RNR). En comunicaciones, mandato o respuesta de enlace de datos que indica una condición temporal de incapacidad para aceptar tramas de entrada.

reconfiguración dinámica (DR). Proceso consistente en cambiar la configuración de una red (las PU y LU periféricas) sin regenerar las tablas de configuración al completo ni desactivar el nodo principal afectado.

recurso. En Nways Switch, elemento de hardware o entidad lógica creados por Control Program. Por ejemplo, los adaptadores, LIC y líneas son recursos físicos. Los puntos de control y conexiones son recursos lógicos.

red. (1) Configuración de software y dispositivos de proceso de datos conectados para el intercambio de información. (2) Grupo de nodos y los enlaces que los interconectan.

red Advanced Peer-to-Peer Networking (APPN). Conjunto de nodos de red interconectados y sus nodos finales clientes.

red APPN. Véase *red Advanced Peer-to-Peer Networking (APPN)*.

red de área amplia (WAN). (1) Red que proporciona servicios de comunicación a un área geográfica mayor

que la servida por una red de área local o una red de área metropolitana, y que puede utilizar o proporcionar recursos públicos de comunicación. (T) (2) Red de comunicación de datos diseñada para servir a un área de cientos o miles de kilómetros; por ejemplo, las redes públicas y privadas de conmutación de paquetes y las redes telefónicas nacionales. (3) Compárese con *red de área local (LAN)* y *red de área metropolitana (MAN)*.

red de área local (LAN). (1) Red de sistema ubicada en el lugar de un usuario dentro de un área geográfica limitada. La comunicación dentro de una red de área local no está sujeta a reglamentos externos; no obstante, la comunicación más allá del límite de una LAN puede estar sujeta a alguna forma de reglamento. (T) (2) Red en la que un conjunto de dispositivos están conectados entre sí para la comunicación y que puede conectarse a una red mayor. (3) Véase también *Ethernet* y *Red en Anillo*. (4) Compárese con *red de área metropolitana (MAN)* y *red de área amplia (WAN)*.

red de área metropolitana (MAN). Red formada por la interconexión de dos o más redes que puede funcionar a una velocidad mayor que éstas, puede atravesar límites administrativos y puede utilizar diversos métodos de acceso. (T) Compárese con *red de área local (LAN)* y *red de área amplia (WAN)*.

red de clase A. En comunicaciones de Internet, red en la que el bit situado más a la izquierda (más significativo) de la dirección IP está establecido en 0 y el identificador de sistema principal ocupa los tres octetos situados más a la derecha.

red de clase B. En comunicaciones de Internet, red en la que los dos bits situados más a la izquierda (más significativo y próximo al más significativo) de la dirección IP están establecidos en 1 y 0, respectivamente, y el identificador de sistema principal ocupa los dos octetos situados más a la derecha.

red de entrada baja (LEN). Posibilidad de los nodos de conectarse directamente entre sí utilizando protocolos básicos de igual a igual para dar soporte a sesiones múltiples y en paralelo entre unidades lógicas.

red de tipo anillo. (1) Red en la que cada nodo tiene exactamente dos ramas conectadas y en la que hay exactamente dos vías de acceso entre dos nodos cualesquiera. (T) (2) Configuración de red en la que los dispositivos están conectados mediante enlaces de transmisión unidireccional para formar una vía de acceso cerrada.

red digital de servicios integrados (RDSI). Red digital de telecomunicaciones de extremo a extremo que da soporte a diversos servicios, los cuales incluyen voz y datos pero no se limitan a ello.

Nota: Las RDSI se utilizan en arquitecturas de red públicas y privadas.

Red en Anillo. (1) Según la norma IEEE 802.5, tecnología de red que controla el acceso al medio pasando una señal (paquete o trama especial) entre las estaciones conectadas al medio. (2) Red FDDI o IEEE 802.5 con una topología de anillo que pasa señales de una estación de anillo de conexión (nodo) a otra. (3) Véase también *red de área local (LAN)*.

red óptica síncrona (SONET). Norma de los EE.UU. para la transmisión de información digital sobre interfaces ópticas. Está estrechamente relacionada con la recomendación sobre la jerarquía digital síncrona (SDH).

red según Red en Anillo. (1) Red de tipo anillo que permite la transmisión de datos unidireccional entre estaciones de datos, mediante un procedimiento consistente en pasar señales, de tal manera que los datos transmitidos vuelven a la estación transmisora. (T) (2) Red que utiliza una topología de anillo, según la cual pasan señales en un circuito de nodo a nodo. Un nodo que está preparado para emitir puede capturar la señal e insertar datos para la transmisión.

red troncal. Red central a la que se conectan redes más pequeñas, casi siempre de menor velocidad. Normalmente, la red troncal tiene una capacidad muy superior a las redes a las que ayuda a interconectarse o es una red de área amplia (WAN), como, por ejemplo, una red pública de datagramas de paquetes conmutados.

reensamblaje. En comunicaciones, proceso consistente en volver a juntar paquetes segmentados después de haberlos recibido.

Registro sin vuelta a cero y con cambios en los unos (NRZ-1). Método de registro donde los unos están representados mediante un cambio en la condición de magnetización y los ceros están representados mediante la ausencia de cambio. Sólo se registran explícitamente las señales de los unos. (Denominado anteriormente registro *sin vuelta a cero invertido*, NRZI.)

Remote Execution Protocol (REXEC). Protocolo que permite la ejecución de un mandato o programa en cualquier sistema principal de la red. El sistema principal local recibe los resultados de la ejecución del mandato.

remoto. (1) Perteneciente a un sistema, programa o dispositivo al que se accede mediante una línea de telecomunicaciones. (2) Sinónimo de *conectado mediante enlace*. (3) Compárese con *local*.

Request for Comments (RFC). En comunicaciones de Internet, serie de documentos que describe una parte del conjunto de protocolos de Internet y experimentos relacionados. Todas las normas de Internet están documentadas como RFC.

resolución de direcciones. (1) Método para correlacionar direcciones de capa de red con direcciones específicas de los medios. (2) Véase también *Address Resolution Protocol (ARP)* y *AppleTalk Address Resolution Protocol (AARP)*.

resolución de nombres. En comunicaciones de Internet, proceso consistente en correlacionar un nombre de máquina con la dirección Internet Protocol (IP) correspondiente. Véase también *Sistema de nombres de dominio (DNS)*.

respuesta a excepción (ER). En SNA, protocolo solicitado en el campo de formato de respuesta solicitado de la cabecera de una petición que indica al receptor que devuelva una respuesta sólo si la petición no es aceptable tal como se recibe o si no puede procesarse; es decir, puede devolverse una respuesta negativa, pero no una respuesta positiva. Compárese con *respuesta definida y sin respuesta*.

restablecimiento. En un circuito virtual, reinicialización del control del flujo de datos. En el restablecimiento, se eliminan todos los datos en tránsito.

ritmo. (1) Técnica mediante la cual un componente de recepción controla la velocidad de transmisión de un componente de emisión para evitar un desbordamiento o una congestión. (2) Véase también *control del flujo*, *ritmo de recepción*, *ritmo de emisión*, *ritmo de nivel de sesión* y *ritmo de ruta virtual (VR)*.

rlogin (inicio de sesión remoto). Servicio ofrecido por los sistemas de Berkeley basados en UNIX que permite que los usuarios autorizados de una máquina se conecten con otros sistemas UNIX en una internet e interactúen como si sus terminales estuvieran conectados directamente. El software rlogin pasa información sobre el entorno del usuario (por ejemplo, el tipo de terminal) a la máquina remota.

Routing Information Protocol (RIP). En el conjunto de protocolos de Internet, protocolo de pasarela interior utilizado para intercambiar información de direccionamiento intradominio y para determinar las rutas óptimas entre los sistemas principales de internet. RIP determina las rutas óptimas sobre la base de la métrica de ruta y no sobre la base de la velocidad de transmisión de un enlace.

Routing Table Maintenance Protocol (RTMP). En redes AppleTalk, protocolo que proporciona generación y mantenimiento de información de direccionamiento en la capa de transporte por medio de la tabla de direccionamiento AppleTalk. La tabla de direccionamiento AppleTalk dirige la transmisión de paquetes por la internet de socket de origen a socket de destino.

RouTing update Protocol (RTP). Protocolo de Virtual NEtworking System (VINES) que mantiene la base de datos de direccionamiento y permite el intercambio de

información de direccionamiento entre nodos VINES. Véase también *Internet Control Protocol (ICP)*.

rsh. Variante del mandato rlogin que invoca un interpretador de mandatos en una máquina remota UNIX y pasa los argumentos de línea de mandatos al interpretador de mandatos saltándose completamente el paso de inicio de sesión.

ruta. (1) Secuencia ordenada de nodos y grupos de transmisión (TG) que representan una vía de acceso de un nodo de origen a un nodo de destino por la que pasa el tráfico intercambiado entre éstos. (2) Vía de acceso que el tráfico de red utiliza para ir del origen al destino.

ruta estática. Ruta entre sistemas principales y/o redes que se entra manualmente en una tabla de direccionamiento.

ruta explícita (ER). En SNA, serie de uno o más grupos de transmisión que conectan dos nodos de subárea. Una ruta explícita se identifica mediante una dirección de subárea de origen, una dirección de subárea de destino, un número de ruta explícita y un número de ruta explícita inversa. Compárese con *ruta virtual (VR)*.

ruta virtual (VR). (1) En SNA, (a) conexión lógica entre dos nodos de subárea que se realiza físicamente como una ruta explícita en particular o (b) conexión lógica contenida en su totalidad dentro de un nodo de subárea para las sesiones intranodo. Una ruta virtual entre nodos de subárea distintos impone una prioridad de transmisión sobre la ruta explícita subyacente, proporciona control del flujo mediante el ritmo de ruta virtual y proporciona la integridad de los datos mediante la numeración en secuencia de las unidades de información de vía de acceso (PIU). (2) Compárese con *ruta explícita (ER)*. Véase también *vía de acceso y extensión de ruta (REX)*.

rutina de carga. (1) Secuencia de instrucciones cuya ejecución hace que se carguen y se ejecuten unas instrucciones adicionales hasta que se haya almacenado todo el programa de sistema. (T) (2) Técnica o dispositivo diseñado para que entre en un estado determinado por medio de su propia acción, por ejemplo, una rutina de máquina cuyas primeras instrucciones sean suficientes para que el resto de la misma entre en el sistema desde un dispositivo de entrada. (A)

S

salto. (1) En APPN, parte de una ruta que no tiene nodos intermedios. Está compuesto por un solo grupo de transmisión que conecta nodos adyacentes. (2) Para la capa de direccionamiento, distancia lógica entre dos nodos en una red.

SAP. Véase punto de acceso a servicios.

segmentación. En OSI, función realizada por una capa para correlacionar una unidad de datos de protocolo (PDU) de la capa a la que da soporte con diversas PDU.

segmento. (1) Sección de cable entre componentes o dispositivos. Un segmento puede estar compuesto por un solo cable provisional, diversos cables provisionales conectados o una combinación de cables provisionales y de construcción conectados. (2) En comunicaciones de Internet, unidad de transferencia entre funciones de TCP en diferentes máquinas. Cada segmento contiene campos de control y de datos; la posición de corriente de bytes actual y los bytes de datos reales se identifican conjuntamente con una suma de comprobación para validar los datos recibidos.

segmento de anillo. Parte de un anillo que puede aislarse (desenchufando conectores) del resto del anillo. Véase *segmento de LAN*.

segmento de LAN. (1) Cualquier parte de una LAN (por ejemplo, un bus o un anillo) que puede funcionar independientemente pero está conectada a otras partes de la red por medio de puentes. (2) Red de tipo bus o anillo sin puentes.

señal. (1) En una red de área local, símbolo de autorización pasado sucesivamente de una estación de datos a otra para indicar la estación que tiene temporalmente el control del medio de transmisión. Cada estación de datos tiene una oportunidad de obtener y utilizar la señal para controlar el medio. Una señal es un mensaje o patrón de bits determinado que significa el permiso para transmitir. (T) (2) En las LAN, secuencia de bits pasada de un dispositivo a otro por el medio de transmisión. Cuando la señal tiene datos añadidos, se convierte en una trama.

Serial Line Internet Protocol (SLIP). Protocolo utilizado sobre una conexión punto a punto entre dos sistemas principales de IP de una línea serie, como, por ejemplo, un cable serie o una conexión RS232 con un módem, de una línea telefónica.

Service Advertising Protocol (SAP). En Internetwork Packet Exchange (IPX), protocolo que proporciona lo siguiente:

- Un mecanismo que permite que los servidores IPX de una internet anuncien sus servicios por el nombre y el tipo. Los servidores que utilizan este protocolo tienen registrados su nombre, tipo de servicios y dirección en todos los servidores de archivos que ejecutan NetWare.
- Un mecanismo que permite que una estación de trabajo difunda una consulta para descubrir las identidades de todos los servidores de todos los tipos, todos los servidores de un tipo específico o el servidor más cercano de un tipo específico.
- Un mecanismo que permite que una estación de trabajo consulte cualquier servidor de archivos que

ejecute NetWare para descubrir nombre y dirección de todos los servidores de un tipo específico.

servicio de directorios (DS). Elemento de servicio de aplicaciones que convierte los nombres simbólicos utilizados por procesos de aplicaciones en direcciones de red completas utilizadas en un entorno de OSI. (T)

servicios de directorios (DS). Componente del punto de control de un nodo APPN que mantiene la información sobre la ubicación de los recursos de red.

servicios de gestión de punto de control (CPMS). Componente de un punto de control que consta de conjuntos de funciones de servicios de gestión y proporciona recursos de ayuda para realizar la gestión de problemas, gestión del rendimiento y de la contabilidad, gestión de los cambios y gestión de la configuración. Las posibilidades proporcionadas por los CPMS incluyen el envío de peticiones a los servicios de gestión de unidad física (PUMS) para probar recursos del sistema, la reunión de información estadística (por ejemplo, datos de errores y del rendimiento) de los PUMS sobre los recursos del sistema y el análisis y presentación de los resultados de las pruebas y la información estadística reunida sobre los recursos del sistema. Las responsabilidades del análisis y de la presentación para la determinación de problemas y la supervisión del rendimiento pueden distribuirse entre los diversos CPMS.

servicios de gestión de SNA (SNA/MS). Servicios proporcionados como ayuda para la gestión de las redes SNA.

servidor. Unidad funcional que proporciona servicios compartidos a estaciones de trabajo sobre una red; por ejemplo, un servidor de archivos, un servidor de impresión, un servidor de correo. (T)

servidor de acceso a red (NAS). Dispositivo que proporciona a los usuarios acceso a red temporal a petición. Este acceso es punto a punto por medio de líneas PSTN o RDSI.

servidor de configuración de emulación de LAN (LECS). Componente de LAN Emulation Service que centraliza y difunde datos de configuración.

servidor de emulación de LAN (LES). Componente de LAN Emulation Service que resuelve destinos de LAN en direcciones ATM.

servidor de informes de configuración (CRS). En el programa Bridge de la Red en Anillo de IBM, el servidor que acepta mandatos del LAN Network Manager (LNM) para obtener información de las estaciones, establecer parámetros de estación y eliminar estaciones de su anillo. Este servidor también recoge y reenvía informes de configuración generados por estaciones de su anillo. Los informes de configuración incluyen los nuevos

informes del supervisor activo y los informes de estación contigua activa de donde proceden los datos (NAUN).

servidor de nombres. En el conjunto de protocolos de Internet, sinónimo de *servidor de nombres de dominio*.

servidor de nombres de dominio. En el conjunto de protocolos de Internet, programa servidor que suministra la conversión de nombres en direcciones correlacionando nombres de dominio con direcciones IP. Sinónimo con *servidor de nombres*.

servidor de puentes de LAN (LBS). En el programa Bridge de la Red en Anillo de IBM, servidor que mantiene la información de estadísticas sobre tramas reenviadas entre dos o más anillos (mediante un puente). El LBS envía estas estadísticas a los gestores de LAN correspondientes mediante el mecanismo de información de LAN (LRM).

servidor de red L2TP (LNS). Un LNS funciona en cualquier plataforma capacitada que pueda ser una estación final de PPP. El LNS maneja la parte del servidor del protocolo L2TP. Puesto que L2TP sólo se apoya en el único medio por el que llegan los túneles de L2TP, el LNS sólo tiene una interfaz LAN o WAN, aunque puede terminar las llamadas que lleguen de cualquier interfaz del rango completo de interfaces PPP soportadas por un LAC. Entre éstas se incluyen la RDSI asíncrona, RDSI síncrona, V.120 y otros tipos de conexiones.

sesión. (1) En la arquitectura de red, con el fin de la comunicación de datos entre unidades funcionales, todas las actividades que tienen lugar durante el establecimiento, mantenimiento y liberación de la conexión. (T) (2) Conexión lógica entre dos unidades de red accesibles (NAU) que puede activarse, adaptarse, para proporcionar varios protocolos y desactivarse de la manera solicitada. Cada sesión está identificada de manera exclusiva en la cabecera de transmisión (TH) que acompaña a cualquier transmisión intercambiada durante la sesión. (3) En L2TP, L2TP crea una sesión cuando se intenta una conexión PPP de extremo a extremo entre un usuario de marcación y los LNS; sin tener en cuenta si el usuario inicia la sesión o si el LNS inicia una llamada hacia fuera. Los datagramas para la sesión se envían por el túnel entre el LAC y el LNS. Los LNS y LAC mantienen la información de estado para cada usuario conectado a un LAC.

Simple Network Management Protocol (SNMP). En el conjunto de protocolos de Internet, protocolo de gestión de red que se utiliza para supervisar direccionadores y redes conectadas. SNMP es un protocolo de capa de aplicación. La información sobre los dispositivos gestionados está definida y almacenada en la base de la información de gestión (MIB) de la aplicación.

simulación. Para los enlaces de datos, técnica mediante la cual un protocolo iniciado en una estación final se reconoce con acuse de recibo y se procesa en un nodo intermedio en nombre del destino final. En la conmutación del enlace de datos del IBM 6611, por ejemplo, las tramas de SNA se encapsulan en paquetes de TCP/IP para el transporte a través de una red de área amplia diferente de SNA, se desempaquetan en otro IBM 6611 y pasan al destino final. Una ventaja de la simulación es que se evitan tiempos de espera excesivos de sesión de final a final.

síncrono. (1) Perteneciente a dos o más procesos que dependen de la aparición de sucesos específicos, como, por ejemplo, señales comunes de temporización. (T) (2) Que se produce con una relación temporal regular o previsible.

sintaxis de abstracción. Especificación de datos que incluye todas las distinciones necesarias en las transmisiones de datos, pero que omite (excluye) otros detalles, como, por ejemplo, los que dependen de las arquitecturas específicas de los sistemas. Véase también *notación de sintaxis de abstracción 1 (ASN.1)* y *normas básicas de codificación (BER)*.

sistema. En el proceso de datos, conjunto de personas, máquinas y métodos organizados para llevar a cabo un conjunto de funciones específicas. (I) (A)

sistema autónomo. En TCP/IP, grupo de redes y direccionadores bajo una sola autorización administrativa. Estas redes y estos direccionadores cooperan estrechamente para propagar la información de asequibilidad (y direccionamiento) de la red entre ellos utilizando un protocolo de pasarela interior de su elección.

sistema de juego reducido de instrucciones (RISC). Sistema que utiliza un juego pequeño y simplificado de instrucciones de uso frecuente para la ejecución rápida.

sistema de nombres de dominio (DNS). En el conjunto de protocolos de Internet, sistema de bases de datos distribuidas utilizado para correlacionar nombres de dominio con direcciones IP.

sistema principal. En el conjunto de protocolos de Internet, sistema final. El sistema final puede ser cualquier estación de trabajo; no es necesario que sea un sistema principal.

socket. (1) Punto final para la comunicación entre procesos o programas de aplicación. (2) Abstracción proporcionada por la Distribución de software de Berkeley de la Universidad de California (software que suele recibir el nombre de UNIX de Berkeley o UNIX de BSD) que funciona como punto final para la comunicación entre procesos o aplicaciones.

sonda de paquetes Internet (PING). (1) En comunicaciones de Internet, programa utilizado en redes TCP/IP para probar la capacidad de alcanzar

destinos enviando a los mismos una petición con eco de Internet Control Message Protocol (ICMP) y esperando una respuesta. (2) En comunicaciones, prueba de asequibilidad.

sondeo. (1) En una conexión multipunto o conexión punto a punto, proceso consistente en invitar a las estaciones de datos a transmitir, una por una. (I) (2) Interrogar a dispositivos con el fin de evitar contenciones, determinar el estado operativo o determinar la disposición para enviar o recibir datos. (A)

soporte de diversos dominios (MDS). Técnica para transportar datos de servicios de gestión entre conjuntos de funciones de servicios de gestión sobre sesiones de LU-LU y CP-CP. Véase también *unidad de mensaje de soporte de diversos dominios (MDS-MU)*.

StreetTalk. En Virtual NETworking System (VINES), sistema exclusivo de denominación y direccionamiento de red amplia que permite que los usuarios ubiquen cualquier recurso de la red y accedan al mismo sin conocer la topología de la red. Véase también *Internet Control Protocol (ICP)* y *RouTing update Protocol (RTP)*.

subárea. Parte de la red SNA compuesta por un nodo de subárea, nodos periféricos conectados y recursos asociados. En un nodo de subárea, todas las unidades de red accesibles (NAU), enlaces y estaciones de enlace adyacentes (de nodos de subárea o nodos periféricos conectados) que son dirigibles dentro de la subárea comparten una dirección de subárea común y tienen direcciones de elementos distintas.

subcapa del control del acceso al medio (MAC). En una red de área local, parte de la capa de enlace de datos que aplica un método de acceso al medio. La subcapa del MAC da soporte a funciones dependientes de la topología y utiliza los servicios de la capa física para proporcionar servicios a la subcapa de control de enlace lógico. (T)

Subnetwork Access Protocol (SNAP). En las LAN, protocolo encargado de establecer diferencias entre protocolos de 5 bytes que identifica la familia de protocolos estándares distintos de IEEE a la que pertenece un paquete. El valor de SNAP se utiliza para diferenciar los protocolos que utilizan \$AA como valor de punto de acceso a servicios (SAP).

subred. (1) En TCP/IP, parte de una red que se identifica mediante una parte de la dirección IP. (2) Sinónimo de *subred (grupo de nodos)*.

subred (grupo de nodos). (1) Cualquier grupo de nodos que tienen un conjunto de características comunes, como, por ejemplo, el mismo identificador de red. (2) Sinónimo con *subred*.

subsistema. Sistema secundario o subordinado que a menudo puede funcionar de manera independiente o asíncrona respecto a un sistema de control. (T)

suma de comprobación. (1) Suma de un grupo de datos que se asocia con el grupo y se utiliza con fines de comprobación. (T) (2) En la detección de errores, función de todos los bits de un bloque. Si las sumas grabadas y las calculadas no coinciden, se indica que hay un error. (3) En un disquete, datos grabados en un sector con fines de detección de errores; una suma de comprobación calculada que no coincide con la suma de comprobación de los datos grabados en el sector indica que hay un sector anómalo. Los datos son numéricos u otras series de caracteres consideradas numéricas con el fin de calcular la suma de comprobación.

supervisor. (1) Dispositivo que observa y registra actividades seleccionadas en un sistema de proceso de datos para el análisis. Sus usos posibles son para indicar cualquier desviación significativa de la norma o para determinar los niveles de utilización de unidades funcionales en particular. (T) (2) Software o hardware que observa, supervisa, controla o verifica operaciones de un sistema. (A) (3) Función necesaria para iniciar la transmisión de una señal del anillo y para proporcionar recuperación de errores de software en el caso de que se pierdan señales, tramas en circulación u otras dificultades. La posibilidad está presente en todas las estaciones de anillo.

supervisor activo. En una Red en Anillo, función realizada en cualquier momento por una estación de anillo que inicia la transmisión de señales y proporciona recursos de recuperación de errores de señales. Cualquier adaptador activo del anillo tiene la posibilidad de proporcionar la función de supervisor activo si falla el supervisor activo actual.

SYNTAX. En el protocolo Simple Network Management Protocol (SNMP), cláusula del módulo de la MIB que define la estructura de datos abstracta correspondiente a un objeto gestionado.

Systems Network Architecture (SNA). Descripción de la estructura lógica, formatos, protocolos y secuencias operativas para la transmisión de unidades de información a través de las redes y para el control de la configuración y del funcionamiento de las mismas. La estructura de capas de SNA permite que los orígenes y destinos finales de la información, es decir, los usuarios, sean independientes de los servicios y recursos de red SNA específicos utilizados para el intercambio de información y que no se vean afectados por dichos servicios y recursos.

T

T1. En los Estados Unidos, línea de acceso público de 1,544 Mbps. Está disponible en veinticuatro canales de 64 Kbps. La versión europea (E1) transmite a 2,048 Mbps.

tabla de correlación de direcciones (AMT). Tabla mantenida en el direccionador AppleTalk que proporciona la correlación actual de las direcciones de nodo con las direcciones de hardware.

tabla de direccionamiento. Conjunto de rutas utilizadas para dirigir el reenvío de datagramas o para establecer una conexión. La información pasa entre direccionadores para identificar la topología de red y la factibilidad de los destinos.

tabla de información de zonas (ZIT). Listado de números de red y sus correlaciones con los nombres de zonas asociadas de internet. Cada direccionador de internet mantiene este listado en una internet AppleTalk.

TCP/IP. (1) Transmission Control Protocol/Internet Protocol. (2) Protocolo de interconexión de sistemas basado en Ethernet/de tipo UNIX que desarrolló originalmente el Departamento de Defensa de los EE.UU. TCP/IP facilitó ARPANET (Advanced Research Projects Agency Network), una red de paquetes conmutados para la investigación en que la capa 4 era TCP y la capa 3, IP.

Telnet. En el conjunto de protocolos de Internet, protocolo que proporciona un servicio de conexión de terminales remotos. Permite que los usuarios de un sistema principal se conecten con un sistema principal remoto e interactúen como usuarios de terminal conectado directamente de este sistema principal.

terminal de datos preparado (DTR). Señal para el módem que se utiliza con el protocolo EIA 232.

tiempo de espera excedido. (1) Suceso que se produce al final de un período predeterminado de tiempo que ha empezado al aparecer otro suceso especificado. (I) (2) Intervalo de tiempo asignado para que tengan lugar determinadas operaciones; por ejemplo, la respuesta a un sondeo o direccionamiento antes de que se interrumpa el funcionamiento del sistema y deba reiniciarse.

topología. En comunicaciones, ordenación física o lógica de los nodos de una red, especialmente las relaciones de un nodo con otro nodo y los enlaces entre los mismos.

trama. (1) En la arquitectura interconexión de sistemas abiertos, estructura de datos perteneciente a un área particular de información y compuesta por ranuras que pueden aceptar los valores de atributos específicos y de las que pueden deducirse inferencias mediante conexiones apropiadas de procedimiento. (T)

(2) Unidad de transmisión en algunas redes de área local, incluida la Red en Anillo de IBM. Incluye delimitadores, caracteres de control, información y caracteres de comprobación. (3) En SDLC, vehículo para cada mandato, cada respuesta y toda información transmitida con procedimientos de SDLC.

trama de información (I). Trama de formato I que se utiliza para la transferencia de información numerada.

trama exploradora. Véase *paquete explorador*.

trama I. Trama de información.

transceptor (transmisor-receptor). En las LAN, dispositivo físico que conecta una interfaz de sistema principal a una red de área local, como, por ejemplo, Ethernet. Los transceptores de Ethernet contienen elementos electrónicos que aplican señales al cable y que detectan colisiones.

Transmission Control Protocol/Internet Protocol (TCP/IP). Conjunto de protocolos de comunicaciones que dan soporte a funciones de conectividad de igual a igual para redes de área local y amplia.

Transmission Control Protocol (TCP). Protocolo de comunicaciones utilizado en Internet y en cualquier red que siga las normas del Departamento de Defensa de los EE.UU. para el protocolo interredes. TCP proporciona un protocolo fiable de sistema principal a sistema principal entre sistemas principales en redes de comunicaciones de paquetes conmutados y en los sistemas interconectados de dichas redes. Utiliza Internet Protocol (IP) como protocolo subyacente.

transporte de vector de gestión de red (NMVT). Unidad de petición/respuesta (RU) de servicios de gestión que fluye sobre una sesión activa entre servicios de gestión de unidad física y servicios de gestión de punto de control (sesión de SSCP-PU).

troncal. (1) En una configuración de anillo de diversos puentes de una red de área local, enlace de gran velocidad al que se conectan los anillos por medio de puentes o direccionadores. Un troncal puede configurarse como bus o como anillo. (2) En una red de área amplia, enlace de gran velocidad al que se conectan nodos o intercambios de conmutaciones de datos (DSE).

túnel. Un túnel está definido mediante un par LNS-LAC. El túnel lleva datagramas de PPP entre el LAC y el LNS. Un solo túnel puede multiplexar muchas sesiones. Una conexión de control que funciona sobre el mismo túnel controla el establecimiento, liberación y mantenimiento de todas las sesiones y del túnel en sí.

U

umbral. (1) En programas puente de IBM, valor asignado al número máximo de tramas que no se

reenvían por un puente debido a errores, antes de que se cuente una aparición de "umbral sobrepasado" y se indique a los programas de gestión de red. (2) Valor inicial a partir del cual un contador disminuye hasta 0 o valor hasta el que aumenta o disminuye un contador a partir de un valor inicial.

unidad básica de transmisión (BTU). En SNA, unidad de datos e información de control que pasa entre los componentes del control de la vía de acceso. Una BTU puede constar de una o más unidades de información de vía de acceso (PIU).

unidad de datos de protocolo de control de enlace lógico (LLC). Unidad de información intercambiada entre estaciones de enlace de diferentes nodos. La unidad de datos de protocolo de LLC contiene un punto de acceso a servicios de destino (DSAP), un punto de acceso a servicios de origen (SSAP), un campo de control y datos de usuario.

unidad de datos de protocolo (PDU). Unidad de datos especificada en un protocolo de una capa determinada y compuesta por información de control de protocolo de esta capa además de, posiblemente, datos de usuario de esta capa. (T)

unidad de información de vía de acceso (PIU). Unidad de mensaje compuesta por una sola cabecera de transmisión (TH) o por una TH seguida de una unidad básica de información (BIU) o un segmento de BIU.

unidad de mensaje de soporte de diversos dominios (MDS-MU). Unidad de mensaje utilizada en el soporte de diversos dominios que contiene datos de servicios de gestión y fluye entre conjuntos de funciones de servicios de gestión sobre las sesiones de LU-LU y CP-CP. Esta unidad de mensaje, así como los datos reales de servicios de gestión que contiene, tiene el formato de corriente de datos general (GDS). Véase también *unidad de servicios de gestión de punto de control (CP-MSU)*, *unidad de servicios de gestión (MSU)* y *transporte de vector de gestión de red (NMVT)*.

unidad de red accesible (NAU). Unidad lógica (LU), unidad física (PU), punto de control (CP) o punto de control de servicios del sistema (SSCP). Es el origen o el destino de la información transmitida por la red de control de la vía de acceso. Sinónimo con *unidad de red direccionable*.

unidad de red direccionable (NAU). Sinónimo de *unidad de red accesible*.

unidad de servicio de canal (CSU). Unidad que proporciona la interfaz a una red digital. La CSU proporciona funciones de acondicionamiento (o igualación) de línea, que mantienen la uniformidad del rendimiento de la señal a lo largo del ancho de banda de canal; remodelación de señal, que constituye la corriente de pulsaciones binarias; y prueba de bucle de

retorno, que incluye la transmisión de señales de prueba entre la CSU y la unidad de canal de oficina de la portadora de red. Véase también *unidad de servicio de datos (DSU)*.

unidad de servicio de datos (DSU). Dispositivo que proporciona una interfaz de servicio de datos digital al equipo terminal de datos de manera directa. La DSU proporciona igualación de bucle y posibilidades de pruebas locales y remotas, así como una interfaz EIA/CCITT estándar.

unidad de servicios de gestión de punto de control (CP-MSU). Unidad de mensaje que contiene datos de servicios de gestión y fluye entre los conjuntos de funciones de servicios de gestión. Esta unidad de mensaje tiene el formato de corriente de datos general (GDS). Véase también *unidad de servicios de gestión (MSU)* y *transporte de vector de gestión de red (NMVT)*.

unidad EIA. Unidad de medida que ha establecido la Electronic Industries Association y es igual a 44,45 milímetros (1,75 pulgadas).

unidad física (PU). (1) Componente que gestiona y supervisa los recursos (como, por ejemplo, enlaces conectados y estaciones de enlace adyacentes) asociados con un nodo tal como lo solicita un SSCP mediante una sesión de SSCP-PU. Un SSCP activa una sesión con la unidad física con el fin de gestionar indirectamente, a través de la PU, recursos del nodo, como, por ejemplo, enlaces conectados. Este término sólo se aplica a los nodos de tipo 2.0, tipo 4 y tipo 5. (2) Véase también *PU periférica* y *PU de subárea*.

unidad lógica (LU). Tipo de unidad de red accesible que permite que los usuarios obtengan acceso a recursos de red y se comuniquen entre sí.

unidad máxima de transmisión (MTU). En las LAN, la mayor unidad de datos posible que puede enviarse por un medio físico determinado en una sola trama. Por ejemplo, la MTU para Ethernet tiene 1500 bytes.

unión de telecomunicaciones internacionales (ITU). Agencia de telecomunicaciones especializada de las Naciones Unidas que se ha establecido con el fin de proporcionar procedimientos y prácticas para la normalización de las comunicaciones, lo cual incluye asignación de frecuencia y regulaciones de la radio universales.

User Datagram Protocol (UDP). En el conjunto de protocolos de Internet, protocolo que proporciona un servicio no fiable de datagramas sin conexiones. Permite que un programa de aplicación de una máquina o proceso envíe un datagrama a un programa de aplicación de otra máquina o proceso. UDP utiliza Internet Protocol (IP) para entregar datagramas.

V

V.34. Recomendación del ITU-T para la comunicación por módem sobre canales estándares de transmisión de voz de 33,6 Kbps (y más lentos) disponibles comercialmente.

V.36. En la comunicación de datos, especificación de la CCITT que proporciona la lista de definiciones para los circuitos de intercambios entre un equipo terminal de datos (DTE) y un equipo de terminación de circuito de datos (DCE) con las velocidades de 48, 56, 64 ó 72 kilobits por segundo.

V.35. En la comunicación de datos, especificación de la CCITT que proporciona la lista de definiciones para los circuitos de intercambios entre un equipo terminal de datos (DTE) y un equipo de terminación de circuito de datos (DCE) con varias velocidades de datos.

V.25. En la comunicación de datos, especificación de la CCITT que define el equipo de respuesta automática y el equipo de llamada automática paralelo de la red telefónica general conmutada, incluidos los procedimientos de inhabilitación de dispositivos controlados con eco para las llamadas establecidas de manera manual y automática.

V.24. En la comunicación de datos, especificación de la CCITT que proporciona la lista de definiciones para los circuitos de intercambios entre un equipo terminal de datos (DTE) y un equipo de terminación de circuito de datos (DCE).

valor por omisión. Perteneciente a un atributo, condición, valor u opción que se supone cuando no se especifica nada de forma explícita. (I)

variable de corriente de datos general (GDS). Tipo de subestructura de RU que va precedida de un identificador y un campo de longitud e incluye datos de aplicación, datos de control de usuario o datos de control definidos según SNA.

variable de la MIB. En el protocolo Simple Network Management Protocol (SNMP), instancia específica de datos definida en un módulo de la MIB. Sinónimo con *objeto de la MIB*.

vector de control de selección de ruta (RSCV). Vector de control que describe una ruta de una red APPN. El RSCV consta de una secuencia ordenada de vectores de control que identifican los TG y nodos que componen la vía de acceso de un nodo de origen a un nodo de destino.

velocidad de información comprometida. Cantidad máxima de datos en bits que la red acepta entregar.

velocidad de transferencia de datos. Promedio de los bits, caracteres o bloques por unidad de tiempo que

pasan entre los miembros del equipo correspondiente en un sistema de transmisión de datos. (I)

Notas:

1. La velocidad se expresa en bits, caracteres o bloques por segundo, minuto u hora.
2. Debe indicarse el equipo correspondiente; por ejemplo, módems, equipo intermedio u origen y destino.

versión. Programa bajo licencia independiente que a menudo tiene un nuevo código o una nueva función significativos.

vía de acceso. (1) En una red, cualquier ruta entre dos nodos cualesquiera. Una vía de acceso puede incluir más de una rama. (T) (2) Serie de componentes de red de transporte (control de la vía de acceso y control de enlace de datos) por los que pasa la información intercambiada entre dos unidades de red accesibles. Véase también *ruta explícita (ER)*, *extensión de ruta* y *ruta virtual (VR)*.

VINES. Virtual NETworking System.

Virtual Networking System (VINES). Sistema operativo de red y software de red de Banyan Systems, Inc. En una red VINES, la función de enlace virtual permite que todos los dispositivos y servicios aparenten estar conectados directamente entre sí cuando en realidad pueden encontrarse a miles de kilómetros de distancia. Véase también *StreetTalk*.

vista de la MIB. En el protocolo Simple Network Management Protocol (SNMP), conjunto de objetos gestionados, conocidos por el agente, que es visible en una comunidad en particular.

vuelco. (1) Datos que se han volcado. (T) (2) Copiar el contenido de la totalidad o de parte del almacenamiento virtual con el fin de reunir información de errores.

X

X.25. (1) recomendación de la comisión consultiva de la telefonía y telegrafía internacionales (CCITT) relativa a la interfaz entre un equipo terminal de datos y las redes de datos de paquetes conmutados. (2) Véase también *conmutación de paquetes*.

X.21. recomendación de la comisión consultiva de la telefonía y telegrafía internacionales (CCITT) relativa a una interfaz de fines generales entre un equipo terminal de datos y un equipo de terminación de circuito de datos para las operaciones síncronas en una red pública de datos.

Xerox Network Systems (XNS). Conjunto de protocolos de internet desarrollados por Xerox Corporation. Aunque es similar a los protocolos TCP/IP,

XNS utiliza unos formatos de paquete y una terminología diferentes. Véase también *Internetwork Packet Exchange (IPX)*.

Z

zona. En redes AppleTalk, subconjunto de nodos dentro de una internet.

Zone Information Protocol (ZIP). En redes AppleTalk, protocolo que proporciona un servicio de gestión de zonas manteniendo una correlación de los nombres de zonas y los números de red de la internet en la capa de sesión.

Índice

Números

2216
definición de sistema principal, actividades
necesarias 367

A

acceso

gestión de cambios

acceso 51

resumen 51

interfaces de canal

consola 431

interfaz de canal

configuración 409

proceso de consola 431

proceso de segundo nivel 14

proceso de tercer nivel 16

protocolo

proceso de configuración 22

proceso de operación (supervisión) 22

acceso a los mandatos de supervisión mp 701

acceso al indicador de configuración mp 697

acceso de soporte técnico 70

acceso de usuario

adición de usuario 83

cambio de contraseña 89

cambio de usuario 90

configuración 70

establecimiento de contraseña 83

listado de información de usuario 100

supresión de usuario 94

activación de interfaces de repuesto 118

activate

mandato GWCON 118

actualización

configuración 12

adaptador de canal

acceso al proceso de consola 431

Canal de diversas vías de acceso+ (MPC+)

bloque de control de Lista de recursos de
transporte (TRL) 385, 386

bloque de control del Nodo principal SNA
local 385, 386

configuración de APPN 402

configuración del sistema principal MVS para
TCP/IP 376

configuración del sistema principal VTAM 385,
386

visión general 400

configuración de interfaz 407

Estación de canal LAN (LCS)

configuración del 2216 391

configuración del sistema principal MVS para
TCP/IP 374

visión general 391

adaptador de canal (*continuación*)

Link Services Architecture (LSA)

bloques de control del sistema principal 381

conexión APPN 396

conexión directa 395

conversión local DLSw 399

visión general 394

mandatos de configuración

add 411

delete 426

list 429, 430

mod 426

resumen 410

set 430

mandatos de supervisión de interfaces

dump_adapter 435

hidtrace 435

list 432

net 434

resumen 431

trace 435

tune 435

mandatos de supervisión de interfaces LCS

resumen 436

mandatos de supervisión de interfaces LSA

list 438

resumen 438

tune 440

mandatos de supervisión de interfaz LCS

list 436

tune 438

mandatos de supervisión de interfaz MPC+

list 441

resumen 441

tune 446

paso a través TCP/IP

configuración del 2216 392

utilización 367

visión general 388

adaptador de canal ESCON

Canal de diversas vías de acceso+ (MPC+)

configuración de TCP/IP 405

configuración de UDP+ 403

configuración 409

adaptador de canal paralelo (PCA)

configuración 409

ejemplo de definición IOCP 371

visión general 388

add

adaptador de canal 411

add 740

mandato CONFIG 77

mandato de configuración ATM 317

mandato de configuración de Interfaz virtual
ATM 323

mandato de configuración de la gestión de
cambios 52

mandato de configuración ELS 158

- add (*continuación*)
 - mandato de configuración Frame Relay 562
 - mandato de configuración SDLC 726
 - mandato de configuración SDLC Relay 710
 - mandato de configuración X.25 485
 - mandato de configuración XTP 519
 - mandato de supervisión SDLC 740
 - mandato de supervisión XTP 526
- adición 17
 - circuito de marcación de entrada
 - ejemplo 17
 - circuito PPP de múltiples enlaces
 - ejemplo 18
- advanced
 - mandato de configuración ELS 158
 - mandato de supervisión ELS 181
- almacenamiento intermedio de mensajes
 - mandatos de configuración ELS 176
 - list 176
 - log 177
 - nolog 177
 - set 178
 - mandatos de supervisión ELS 206
 - flush 207
 - list 207
 - log 207
 - nolog 208
 - read-file 209
 - set 209
 - tftp 210
 - view 211
 - write-buffer 212
 - visión general 153
- análisis de problemas 388
- análisis y resolución de problemas 388
- anotación cronológica de sucesos
 - subsistema 139
- anotación cronológica remota
 - consideraciones adicionales 152
 - anotación cronológica duplicada 152
 - mensajes que contienen direcciones IP 152
 - números de secuencia repetidos 153
 - ejemplos de salida 149
- AppleTalk Control Protocol
 - para PPP 633
- APPN
 - bucle de retorno LA, configuración 425
 - LSA
 - configuración del 2216 391
 - configuración del sistema principal VTAM 382
 - IBM 2216, configuración 396
- APPN HPR Control Protocol
 - para PPP 636
- APPN ISR Control Protocol
 - para PPP 636
- archivo de carga del direccionador
 - creación a partir de múltiples discos 823
 - desensamblaje bajo DOS 824
 - desensamblaje bajo UNIX 825
 - ensamblaje bajo DOS 823
 - ensamblaje bajo UNIX 823
- archivo de definición de nodo principal conmutado, ejemplos
 - bloque de control VTAM 382
 - conexión LSA APPN en el sistema principal VTAM 383
 - conexión LSA directa en el sistema principal VTAM 382
 - conexión LSA DLSw en el sistema principal VTAM 383
 - conversión local LSA DLSw en el sistema principal VTAM 384
- archivo de definición de nodo principal XCA, ejemplos
 - bloque de control VTAM 381
 - conexión LSA APPN en el sistema principal VTAM 382
 - conexión LSA directa en el sistema principal VTAM 382
 - conexión LSA DLSw en el sistema principal VTAM 383
 - conversión local LSA DLSw en el sistema principal VTAM 384
- archivo de inicialización ATCSTRxx, para VTAM 386
 - listado, recuperación y supresión 124
- ARP configuration
 - config 336
 - list 337
 - remove 337
 - set 337
- ATCSTRxx, archivo de inicialización de VTAM 386
- ATM
 - cómo entrar direcciones 311
- atm-llc
 - mandatos de supervisión ATM 324
- atributos, remotos AAA 827
- atributos AAA, remotos 827
- atributos remotos AAA 827
 - palabras clave 828
 - radius 827
 - TACACS 831
- autenticación
 - configuración de interfaz PPP 630
 - dispositivo remoto
 - configuración de interfaz PPP para utilizar 631
- autenticación PAP para PPP 629
- ayuda
 - mandato console 11
- ayuda en línea 24, 26

B

- Banyan VINES Control Protocol (BVCP)
 - para PPP 633
- base de datos de configuración de arranque
 - visualización 57
- BCM 304
 - soporte para el puente de ruta de origen 306
 - Soporte para IP 304
 - Soporte para IPX
 - BCM IPX Server Farm 305
 - impedir que un LEC se trate como 305
 - soporte para NetBIOS 305

BCM 304 (*continuación*)
 Compartimiento de nombres de NetBIOS 306
 BCM IPX Server Farm
 impedir que un LEC se trate como 305
 beneficios de LAN Emulation 291
 bloque de control de Lista de recursos de transporte
 (TRL) 385, 386, 387
 bloque de control del Nodo principal SNA local 385,
 386
 boot
 mandato CONFIG 84
 Boot CONFIG
 proceso
 entrada desde CONFIG 84
 Bridging Control Protocol (BCP)
 para PPP 633
 Broadcast and Unknown Server 293, 302
 broadcast manager 304
 bucle de retorno, APPN, configuración 425
 buffer
 mandato GWCON 119
 BUS 291, 293
 conexión a 302
 funciones de 302

C

callback
 mandato de supervisión de circuito de
 marcación 804
 Callback Control Protocol (CBCP)
 para PPP 634
 calls
 mandato de supervisión RDSI 790
 mandatos de supervisión V.25bis 760
 canal de bucle de retorno APPN
 reconfiguración dinámica 457
 Canal de diversas vías de acceso+ (MPC+)
 configuración
 sistema principal MVS para TCP/IP 376
 configuración de APPN 402
 configuración de TCP/IP 405
 configuración de UDP+ 403
 configuración del sistema principal VTAM 385, 386
 interfaz virtual, configuración 418
 subcanal, configuración 420
 visión general 400
 Canal de diversas vías de acceso (MPC+)
 list, mandato de supervisión de interfaces 441
 mandatos de supervisión de interfaz MPC+
 tune 446
 resumen, mandatos de supervisión de
 interfaces 441
 canal ESCON
 reconfiguración dinámica 447
 canal LCS
 reconfiguración dinámica 453
 canal LSA
 reconfiguración dinámica 451
 canal MPC
 reconfiguración dinámica 455

canal PCA
 reconfiguración dinámica 449
 carácter de interceptación 11
 cambio 37
 características
 acceso a los procesos de configuración y
 consola 21
 carga
 a una hora específica 49
 cierre de una conexión telnet 43
 cifrado
 configuración 660
 CIR
 CIR de circuito virtual permanente huérfano 543
 relación con VIR 545
 supervisión 545, 546
 circuito de marcación de entrada
 ejemplo de add device 17
 circuitos de marcación
 adición 752, 779
 configuración 753, 780
 configuración para MP 693
 RDSI 770
 circuitos de marcación de entrada
 conexiones virtuales (VC) 636
 configuración 637
 consideraciones 636
 circuitos virtuales conmutados Frame Relay (SVC) 533
 adición 567
 cambio 572
 eliminación 593
 listado 590, 591, 611, 612
 circuitos virtuales conmutados huérfanos
 Frame Relay 537
 circuitos virtuales permanentes (PVC) Frame Relay
 cambio 572
 circuitos virtuales permanentes huérfanos
 Frame Relay 536
 circuits
 mandato de supervisión RDSI 790
 mandatos de supervisión V.25bis 761
 clear
 mandato CONFIG 91
 mandato de configuración ELS 158
 mandato de supervisión ELS 181
 mandato de supervisión Frame Relay 600
 mandato de supervisión PPP 662
 mandato GWCON 120
 mandatos de supervisión SDLC 740
 clear-counters
 mandato de supervisión LLC 255
 clear-port-statistics
 mandato de supervisión SDLC Relay 718
 CLLM
 descripción de 543
 códigos de terminación de paquetes 140
 colas Frame Relay
 listado 611
 collisions
 mandato de supervisión de Ethernet de 10/100
 Mbps 289

- collisions (*continuación*)
 - mandato de supervisión Ethernet 270
- cómo listar los protocolos 105
- comodines, dirección DTE 508
- comodines de dirección DTE 508
- componentes de LAN Emulation 292
- conexión a un proceso 9
- conexión al BUS 302
- conexión directa, LSA, configuración 395
- conexión DLSw
 - configuración
 - 2216 397
 - conversión local en el 2216 399
 - sistema principal VTAM 383, 384
 - LSA 397, 399
- conexiones SDLC
 - soporte para 726
- conexiones telnet 5
 - cierre 43
 - obtención del estado de 43
- conexiones virtuales (VC)
 - configuración 637
 - consideraciones 636
 - visión general 636
- configuración
 - acceso al indicador mp 697
 - acceso de usuario 70
 - actualización 12
 - actualización de la memoria 115
 - adaptador de canal ESCON 409
 - adaptador de canal paralelo (PCA) 409
 - APPN
 - bucle de retorno 425
 - basándose en una existente 12
 - cifrado 660
 - conexiones virtuales (VC) 637
 - DECnet 817
 - FDDI 243
 - interfaces de red 19
 - interfaz de adaptador de canal
 - acciones necesarias 407
 - add 411
 - interfaz de canal
 - delete 426
 - list, mandato 429, 430
 - mod, mandato 426
 - resumen de mandatos 410
 - set, mandato 430
 - interfaz multilink PPP 693
 - en circuitos de marcación 693
 - en enlaces serie 694
 - en redes con túneles de capa 2 694
 - para MP de múltiples chasis 695
 - IP 813
 - IPX 814
 - LCS
 - interfaz virtual 411
 - subcanal 412
 - LSA
 - conexión APPN 396
 - conexión directa 395
- configuración (*continuación*)
 - LSA (*continuación*)
 - conexión directa en el sistema principal
 - VTAM 382
 - conexión DLSw en el 2216 397
 - conversión local DLSw en el 2216 399
 - interfaz virtual 414
 - subcanal 416
 - llamada de retorno PPP 631
 - mandato network, adaptador de canal 410
 - mandatos de acceso 407
 - MPC+ 402, 403, 405
 - interfaz virtual 418
 - subcanal 420
 - OPCON 33
 - paso a través TCP/IP 392
 - primera 11
 - reconfiguración 388
 - sistema principal
 - necesaria para definir la conexión 367
 - planificación de la definición 367
 - sistema principal MVS para TCP/IP 374
 - sistema principal VTAM
 - conexión APPN 382
 - conexión DLSw 383
 - MPC+ 385, 386
 - sugerencias 11
 - visión general 367
 - XTP 519
 - configuración basándose
 - en existente 12
 - configuración de interfaces de repuesto 71
 - activación 118
 - configuración 71
 - definición 220
 - restricciones 72
 - configuración de la versión de señalización en LAN Emulation 295
 - Configuración de valores distintos de automático para dúplex 281
 - configuración ELS
 - entrada y salida 138
 - configuración rápida 8, 14
 - configuración de la función de puente 811
 - configuración de protocolos
 - interfaz de usuario IP 813
 - interfaz de usuario IPX 815
 - procedimiento 812
 - descripción 69
 - Configuraciones que pueden resultar en anomalía de la activación del enlace 281
 - Configuraciones que pueden resultar en discrepancias de las modalidades de dúplex durante el funcionamiento 282
 - configuration
 - mandato GWCON 120
 - mandato OPCON 16, 34
 - visualización de información acerca de 120
 - Congestión de circuitos 546
 - respuesta con moderación de la velocidad 546
 - conjunto de datos de configuración de E/S 368

- connector-Type
 - mandato de configuración Ethernet 268
- consideraciones
 - conexiones virtuales (VC) 636
 - multilink PPP protocol (MP) 692
- consolas de dispositivo
 - local 3
 - remotas 4
 - utilización 3
- consolas locales 3
- consolas remotas 4
- console
 - mandato OPCON 34
- Consulta de configuración rápida 810
- contención de circuitos
 - RDSI 771
- contraseña, establecimiento para usuario 83
- contraseñas 5
- Control de flujo
 - paquetes 120
- coprocesador
 - acceso al proceso de configuración 16
- copy
 - mandato de configuración de la gestión de cambios 52
- CPU
 - visualización del uso de memoria de 127
- create
 - mandatos de configuración de filtros de red ELS 174
 - mandatos de supervisión de filtros de red ELS 204
- cronometraje y tipo de cable 459

CH

- change
 - mandato CONFIG 84
 - mandato de configuración Frame Relay 571
 - mandato de configuración X.25 492
 - mandato de configuración XTP 522
- channels
 - mandato de supervisión RDSI 790
- CHAP
 - autenticación para PPP 629
 - configuración 640
 - supervisión 662

D

- DDN
 - valores por omisión 821
- DECnet, configuración 817
- DECnet Control Protocol (DNCP) para PPP 634
- default
 - mandato de configuración ELS 159
- definición del 2216
 - en el sistema operativo 372
- delete
 - adaptador de canal 426
 - delete 740
 - mandato CONFIG 93

- delete (*continuación*)
 - mandato de configuración de circuito de marcación 798
 - mandato de configuración ELS 159
 - mandato de configuración SDLC 728
 - mandato de configuración SDLC Relay 712
 - mandato de configuración X.25 493
 - mandato de configuración XTP 522
 - mandato de supervisión SDLC 740
 - mandato de supervisión XTP 527
 - mandatos de configuración de filtros de red ELS 175
 - mandatos de supervisión de filtros de red ELS 205
 - RDSI 93
- describe
 - mandato de configuración de la gestión de cambios 54
- descripción de OPCON 33
- diags
 - mandato OPCON 35
- direccionador
 - visualización de información acerca de 97
- direccionamiento ATM 293
- direccionamiento dinámico
 - OSPF 814
 - RIP 814
- direcciones
 - RDSI 771
- direcciones, entrada
 - ATM 311
- direcciones ATM de componentes de LAN Emulation 294
- disable
 - compresión de datos 640
 - conexión de establecimiento de enlace SDLC 740
 - Lower DTR 640
 - mandato CONFIG 94
 - mandato de configuración ATM 322
 - mandato de configuración de la gestión de cambios 55
 - mandato de configuración del rendimiento 214
 - mandato de configuración Frame Relay cir-monitor 572
 - mandato de configuración SDLC 728
 - mandato de configuración SDLC Relay 712
 - mandato de configuración X.25 476
 - mandato de configuración XTP 524
 - mandato de supervisión del rendimiento 215
 - mandato de supervisión Frame Relay 601
 - mandato de supervisión SDLC Relay 718
 - mandato GWCON 123
 - mandatos de configuración de filtros de red ELS 175
 - mandatos de supervisión de filtros de red ELS 205
 - multilink protocol 640
 - protocolos de autenticación 640
- disable-completion
 - mandato CONFIG 94
- disk
 - mandato GWCON 124

- display
 - mandato de configuración ELS 159
 - mandato de supervisión ELS 182
- dispositivo
 - rearranque 39
 - salir 6
 - visualización de estadísticas de hora acerca de 133
 - volver a cargar 6, 15
- dispositivo, volver a cargar 819
- dispositivo de interfaz
 - adición 77
 - cambio 84
- dispositivo remoto
 - autenticación
 - configuración de interfaz PPP para 630
 - configuración de interfaz PPP para utilizar 631
- distintivos HDLC
 - en trama Frame Relay 539
- divert
 - mandato OPCON 35
- DLCI (Identificador de conexión de enlace de datos)
 - Frame Relay 532
- DOS
 - desensamblaje de un archivo de carga 824
 - ensamblaje de un archivo de carga 823
- DTE remoto, búsqueda de 508
- dump
 - mandato de supervisión de Red en Anillo 225
 - mandato de supervisión de Red en Anillo Rápida 234
- dump_adapter, mandato de supervisión de interfaces de canal 435
- duplex
 - mandato de configuración Ethernet 286

E

- ejemplo, configuración rápida 810
- ejemplo de add device
 - PPP de múltiples enlaces 18
- ejemplos
 - archivo de definición de nodo principal conmutado
 - bloque de control VTAM 382
 - conexión LSA APPN en el sistema principal VTAM 383
 - conexión LSA directa en el sistema principal VTAM 382
 - conexión LSA DLSw en el sistema principal VTAM 383
 - conversión local LSA DLSw en el sistema principal VTAM 384
 - archivo de definición de nodo principal XCA
 - bloque de control VTAM 381
 - conexión LSA APPN en el sistema principal VTAM 382
 - conexión LSA directa en el sistema principal VTAM 382
 - conexión LSA DLSw en el sistema principal VTAM 383
 - conversión local LSA DLSw en el sistema principal VTAM 384

- ejemplos (*continuación*)
 - definición del 2216 en HPDT UDP para MVS o VM 381
 - definición del 2216 en TCP/IP para MVS o VM para el LCS 377
 - definición del 2216 en TCP/IP para MVS o VM para MPC+ 379
- IOCP
 - definición para canal ESCON 368
 - definición para el adaptador de canal paralelo 371
 - definición para el sistema principal EMIF 369
- els
 - mandato OPCON 36
- ELS
 - almacenamiento intermedio de mensajes
 - visión general 153
 - anotación cronológica remota
 - anotación cronológica duplicada 152
 - consideraciones adicionales 152
 - mensajes que contienen direcciones IP 152
 - números de secuencia repetidos 153
 - salida 149
 - captura de la salida utilizando Telnet 142
 - cómo utilizar 141
 - conceptos de 138
 - configuración de las rupturas 143
 - descripción de 137
 - detección 193, 200
 - ejemplo 1 de resolución de problemas 144
 - ejemplo 2 de resolución de problemas 144
 - ejemplo 3 de resolución de problemas 144
 - entrada 96
 - guardar 191
 - interpretación de mensajes 139
 - rastreo 170, 194
 - remote-logging 167, 191
 - supervisión 157
 - utilización para resolver problemas 143
 - volver a cargar 191
- EMIF
 - ejemplo de definición IOCP 369
- emulación de LAN 291
 - beneficios 291
 - Broadcast and Unknown Server (BUS) 293
 - Broadcast Manager (BCM) 304
 - BUS 293
 - cliente 292
 - componentes 292
 - componentes, direcciones ATM de 294
 - conexión al BUS 302
 - conexión al LES 300
 - configuración de la versión de señalización 295
 - direccionamiento ATM para 293
 - direccionamiento en ATM 293
 - direcciones ATM de componentes de LAN
 - Emulation 294
 - establecimiento de una VCC de datos directos 303
 - fiabilidad 306
 - funciones de ILMI, relacionadas 295
 - funciones del BUS 302

- emulación de LAN 291 *(continuación)*
 - LAN Emulation Configuration Server, visión general de 296
 - LECS, políticas y valores de políticas 297
 - LECS, visión general de 296
 - localización de LECS utilizando ILMI 295
 - parámetros clave de configuración 309
 - política de destino LAN del LECS (política de dirección MAC) 298
 - política de nombre de ELAN 298
 - política de tamaño máximo de trama 299
 - política de tipo de ELAN 299
 - políticas de asignación de ejemplo para el LECS 298
 - redundancia 306
 - registro de direcciones en el LES 301
 - resolución de direcciones por el LES 301
 - seguridad 308
 - servidor 292
 - servidor de configuración 292
 - servidor de configuración, políticas y valores de políticas 297
 - TLV de LECS 300
 - valores de política de duplicados 299
 - versión de señalización 295
 - visión general 291
 - visión general de funciones de ILMI relacionadas 295
 - visión general de las extensiones del direccionador para LAN Emulation 304
- enable
 - compresión de datos 642
 - CHAP 642
 - Lower DTR 642
 - mandato CONFIG 95
 - mandato de configuración ATM 321
 - mandato de configuración de la gestión de cambios 55
 - mandato de configuración del rendimiento 214
 - mandato de configuración Frame Relay 576
 - mandato de configuración SDLC 728
 - mandato de configuración SDLC Relay 712
 - mandato de configuración X.25 475
 - mandato de configuración XTP 524
 - mandato de supervisión del rendimiento 215
 - mandato de supervisión Frame Relay 601
 - mandato de supervisión SDLC 741
 - mandato de supervisión SDLC Relay 719
 - mandato GWCON 124
 - mandatos de configuración de filtros de red ELS 175
 - mandatos de supervisión de filtros de red ELS 206
 - multilink protocol 642
 - PAP 642
 - protocolos de autenticación 642
- Enable-completion
 - mandato CONFIG 95
- enable lmi 598
- encapsulador
 - mandato de configuración de circuito de marcación 798
- enlaces PPP serie
 - configuración para MP 694
- entidades de gestión LMI 541
- entorno, nivel inferior
 - salir 11
- entorno de configuración ELS
 - entrada y salida 157
- entorno de consola ELS
 - anotación cronológica remota 145
 - anotación cronológica remota de 2216 configuración 147
 - estación de trabajo remota configuración 146
 - nivel
 - definido 145
 - recurso de anotación cronológica del sistema definido 145
- entorno operativo ELS
 - entrada y salida 180
- erase
 - mandato de configuración de la gestión de cambios 56
- error
 - mandato GWCON 125
- ESCON
 - visión general 388
- ESI 293
- establecimiento y cambio de la hora, fecha y reloj 114
- Estación de canal de LAN (LCS)
 - emulación 3172 411
 - interfaz virtual, configuración 411
 - mandatos de supervisión de interfaz LCS
 - list 436
 - resumen 436
 - tune 438
 - subcanal, configuración 412
- Estación de canal LAN (LCS)
 - configuración 2216 391
 - sistema principal MVS para TCP/IP 374
 - visión general 391
- estadísticas
 - borrado 120
- Ethernet
 - interfaz de red
 - configuración 267
 - interfaz de red de 10/100 Mbps
 - configuración 285
 - tipo de encapsulación 816
 - tipos de encapsulación para IPX 816
 - visualización de estadísticas 263
 - visualización de estadísticas de 10/100 Mbps 273
- event
 - mandato CONFIG 96
 - mandato GWCON 126
 - mandato OPCON 36
- Evitación explícita de congestión hacia adelante 547
- Evitación explícita de congestión hacia atrás 547
- exit
 - mandato de configuración de Ethernet de 10/100 Mbps 288

extensiones del direccionador para LAN
Emulation 304

F

FDDI

configuración 243
GWCON 247

FDDI (Fiber Distributed Data Interface)

utilización 239

FDDI y GWCON 247

features 96

filtro MAC 126
Filtro MAC 96
Función de servidor fino 96
mandato CONFIG 96
mandato GWCON 126
reserva de ancho de banda 126
Reserva de ancho de banda 96
restauración de WAN 126
Restauración/redireccionamiento de WAN 96
Subsistema de codificación 96

fecha, establecimiento y cambio 114

fiabilidad de LAN Emulation 306

Fiber Distributed Data Interface

protocolos soportados 239
visión general 239

files

mandato de supervisión ELS 182

filter

mandato de configuración ELS 160
mandato de supervisión ELS 183

flush

mandato OPCON 36

Frame Relay 535

acceso a la configuración 558
AR estático 566
circuitos virtuales 531
circuitos virtuales conmutados huérfanos 537
circuitos virtuales permanentes 535
circuitos virtuales permanentes huérfanos 536
configuración 558, 561
correlación de direcciones de protocolo 540
datos de usuario 539
dirección extendida 539
distintivos HDLC 539
DLCI (Identificador de conexión de enlace de datos) 532
elegibilidad para eliminar 539
emulación de multidifusión 541
entidades de gestión LMI 541
formato de trama 538
gestión de red 541
grupos necesarios 537
habilitación de la gestión de PVC 559
habilitación de la gestión de SVC 560
Identificador de conexión de enlace de datos (DLCI) 539
información variable de información (VIR) 545
informe del estado de la gestión 542
descripción 542
informe de estado completo 542

Frame Relay 535 (continuación)

informe del estado de la gestión 542
(continuación)
informe de verificación de la integridad del enlace 542

inicialización de interfaz 535

interfaz de red 561, 615

introducción 531

mandato/respuesta 539

Notificación explícita de congestión hacia adelante 539

Notificación explícita de congestión hacia atrás 539

notificación y evitación de la congestión 547

protocolo de enlace de datos LAPD 531, 538

PVC manejadores de tramas 534

PVC y 537

red 532

reenvío de tramas descrito 540

Reserva de ancho de banda 551

subinterfases 533

SVC

FRF 4 542

tamaño de exceso de ráfaga 544

utilización 531

velocidad de información de circuito 543

velocidad de línea 545

velocidad máxima de información 545

velocidad mínima de información 545

velocidad variable de información 545

velocidades de datos 543

Frame Relay Forum Implementation Agreement 4 (FRF 4) 542

función de puente

a través de LCS

parámetros 392

función de puente, configuración utilizando la configuración rápida 811

función de similar de reserva, XTP 508

funciones de ILMI en LAN Emulation 295

funciones del BUS 302

G

gestión de cambios

acceso 51

comprensión 47

configuración 51

mandatos disponibles desde 51

modelos 47

gestión de capa de enlace consolidada (CLLM)

descripción de 543

grupo

supresión 159

grupos de usuarios cerrados

alteración temporal del cug 0 467

configuración 467

establecimiento de circuitos X.25 466

extendidos

tipos de 466

soporte XTP

visión general 509

visión general 465

- grupos de usuarios cerrados bilaterales
 - visión general 466
- GTE-Telenet
 - valores por omisión 821
- GWCON
 - FDDI 247
 - mandatos
 - interfaz SDLC 749
 - interfaz X.25 501
 - proceso
 - entrada 15
- GWCON y FDDI 247

H

- halt
 - mandato OPCON 37
- HCD
 - definición MVS/ESA 373
 - programa 367
- hidtrace, mandato de supervisión de interfaces de canal 435
- histórico de mandatos 26, 27
- hora
 - carga de imagen activada 49
 - establecimiento y cambio 114
- HPDT UDP
 - definición del 2216 para MVS o VM, ejemplo 381
- HSSI
 - set
 - cable 595, 652
 - clocking 596
 - crc-type 594
 - cronometraje 653
 - tipo crc 596
 - valores por omisión de congestión del circuito 595
 - velocidad de línea 598

I

- IBM 2216
 - modalidad de Sólo configuración 68
- identificación de indicadores 10
- Identificador de conexión de enlace de datos (DLCI)
 - Frame Relay 532, 539
- identificador del sistema final 293
- imagen
 - carga a una hora específica 49
- indicador, supervisión, visualización 431
- indicador de configuración multilink protocol (mp)
 - acceso 697
- indicadores
 - CONFIG 10
 - GWCON 10
 - identificación 10
 - OPCON 10
 - procesos de dispositivo 10
- inicio de sesión
 - desde consola local 5
 - desde consola remota 5
 - inhabilitación 94

- inicio de sesión (*continuación*)
 - nombre de inicio de sesión remoto 5
- inicio de sesión remoto 5
- intercept
 - mandato OPCON 37
- interface
 - mandato de configuración ATM 316
 - mandato GWCON 126
 - mandatos de supervisión ATM 324, 325, 327
- interfaces
 - configuración de repuesto 71
 - de repuesto 220
- interfaces, restricciones 72
- interfaces de línea serie
 - configuración 459
- interfaces de punto a punto
 - configuración 639
- interfaces de Red en Anillo
 - configuración 221
- interfaces de red LLC
 - configuración 251
- interfaces X.25
 - grupos de usuarios cerrados
 - alteración temporal del proceso para el cug 0 467
 - configuración 467
 - establecimiento de circuitos 466
 - tipos extendidos 466
 - visión general 465
 - grupos de usuarios cerrados bilaterales
 - visión general 466
- interfaz
 - lista de procesos 6
 - usuario 6
- interfaz de línea serie
 - acceso al proceso de configuración 459
- interfaz de llamada de entrada SDLC conmutada
 - configuración 723
- interfaz de red
 - acceso al proceso de configuración 16
 - acceso al proceso de consola 20
 - configuración 16, 219
 - habilitación 132
 - inhabilitación 123
 - interfaces soportadas 19
 - mandato interface de GWCON 219
 - proceso de consola 16, 219
 - SDLC 749
 - supervisión 21, 219
 - supresión 93
 - verificación 132
 - visualización de información acerca de 97, 120, 126
 - visualización de la configuración 19
 - X.25 501
- Interfaz de red a red de LAN Emulation (LNNI) 309
- interfaz de red ATM
 - supervisión 315
 - utilización 311
- interfaz de Red en Anillo
 - estadísticas visualizadas para 226

- interfaz de Red en Anillo Rápida
 - estadísticas visualizadas para 235
 - interfaz de red Ethernet
 - utilización 263
 - interfaz de red Ethernet de 10/100 Mbps
 - configuración de valores distintos de automático para dúplex 281
 - Configuraciones que pueden resultar en anomalía de la activación del enlace 281
 - Configuraciones que pueden resultar en discrepancias de las modalidades de dúplex durante el funcionamiento 282
 - negociación automática en la interfaz Ethernet de 10/100 Mbps 281
 - utilización 273
 - Interfaz de red punto a punto
 - utilización 621
 - interfaz de red X.25
 - acceso al proceso de supervisión 497
 - configuración 469
 - personalidad nacional 462, 821
 - statistics 501
 - utilización 461
 - interfaz de usuario
 - procesos 6
 - software 6
 - interfaz OPCON
 - configuración 33
 - interfaz RDSI
 - utilización 769
 - Interim Local Management Interface 295
 - IOCDs 368
 - IOCP
 - definiciones 368
 - ejemplo de definición para canal ESCON 368
 - ejemplo de definición para el adaptador de canal paralelo 371
 - IP, configuración 813
 - IP (Internet Protocol), configuración utilizando la configuración rápida 813
 - IP Control Protocol (IPCP)
 - para PPP 634
 - ip-encapsulation
 - mandato de configuración Ethernet 268, 338
 - mandato de configuración Ethernet de 10/100 Mbps 286
 - IPv6 Control Protocol (IPv6CP)
 - para PPP 635
 - IPX, configuración 814
 - IPX (Internetwork Packet Exchange)
 - configuración utilizando configuración rápida 815
 - tipos de encapsulación de red en anillo 815
 - tipos de encapsulación Ethernet 816
 - IPX Control Protocol (IPXCP)
 - para PPP 635
- L**
- L2_Counters
 - mandato de supervisión RDSI 792
 - L3_Counters
 - mandato de supervisión RDSI 792
 - LAN emulation client--consulte LEC 364
 - LAN Emulation Client (LEC) 331
 - configuración 331, 333
 - LAN Emulation Configuration Server 296
 - LAN Emulation Server 300
 - LCS
 - emulación 3172 393
 - función de puente
 - parámetros 392
 - LE Client 292
 - LE-Client
 - mandato de configuración ATM 315
 - LE-Services
 - mandato de configuración ATM 315
 - LEC conforme a forum
 - ARP configuration 335
 - configuración de un cliente específico 334
 - LECS 291
 - componente de LAN Emulation 296
 - política de destino LAN (política de dirección MAC) 298
 - política de nombre de ELAN 298
 - política de tamaño máximo de trama 299
 - política de tipo de ELAN 299
 - políticas de asignación de ejemplo 298
 - TLV 300
 - valores de política de duplicados 299
 - y extensiones LAN 296
 - y LAN Emulation 292
 - LES 291, 292
 - conexión a 300
 - registro de direcciones 301
 - resolución de direcciones 301
 - Link Control Protocol (LCP)
 - paquetes 625
 - relación con PPP 624
 - Link Services Architecture (LSA)
 - conexión APPN
 - configuración del 2216 396
 - configuración del sistema principal VTAM 382
 - conexión directa
 - configuración del 2216 395
 - en el sistema principal VTAM, configuración 382
 - conexión DLSw
 - configuración del 2216 397, 399
 - configuración del sistema principal VTAM 383, 384
 - interfaz virtual, configuración 414
 - mandatos de supervisión de interfaces LSA
 - list 438
 - resumen 438
 - tune 440
 - sistema principal
 - bloques de control 381
 - subcanal, configuración 416
 - visión general 394
 - list 22
 - adaptador de canal
 - mandato de configuración 429, 430

- list 22 *(continuación)*
 - mandato de supervisión de interfaces 432
- list 741
- mandato CONFIG 97
- mandato de configuración ATM 317
- mandato de configuración de circuito de
 - marcación 799
- mandato de configuración de Interfaz virtual
 - ATM 323
- mandato de configuración de la gestión de
 - cambios 57
- mandato de configuración de Red en Anillo 221
- mandato de configuración de Red en Anillo
 - Rápida 232
- mandato de configuración del rendimiento 214
- mandato de configuración ELS 160
- mandato de configuración Ethernet 268
- mandato de configuración Ethernet de 10/100
 - Mbps 287
- mandato de configuración Frame Relay 583
- mandato de configuración LLC 351
- mandato de configuración Point-to-Point 644
- mandato de configuración RDSI 784
- mandato de configuración SDLC 729
- mandato de configuración SDLC Relay 713, 714
- mandato de configuración V.25bis 756
- mandato de configuración X.25 494
- mandato de configuración XTP 524
- mandato de supervisión ATM LLC 328
- mandato de supervisión de interfaces LCS 436
- mandato de supervisión de interfaces MPC 441
- mandato de supervisión de interfaz LSA 438
- mandato de supervisión del LEC 354
- mandato de supervisión del rendimiento 216
- mandato de supervisión ELS 183
- mandato de supervisión Frame Relay 601
- mandato de supervisión LLC 255, 363
- mandato de supervisión PPP 662
- mandato de supervisión SDLC 741
- mandato de supervisión SDLC Relay 719
- mandato de supervisión X.25 498
- mandato de supervisión XTP 527
- mandatos de configuración de filtros de red
 - ELS 176
- mandatos de supervisión ATM 325
- mandatos de supervisión de filtros de red ELS 206
- list devices 315
- list devices, mandato 18, 267, 285, 409, 639, 755
- lista
 - adaptador de canal
 - mandato de configuración de interfaz 410
- listado de la configuración 105
- LNNI 309
- load
 - mandato CONFIG 101
- localización de LECS utilizando ILMI 295
- lock
 - mandato de configuración de la gestión de
 - cambios 58
- logout
 - mandato OPCON 37

LL

- llamada de retorno PPP
 - configuración 631
- llc
 - mandato de configuración de Red en Anillo 222
 - mandato de configuración de Red en Anillo
 - Rápida 232
 - mandato de configuración Point-to-Point 649
 - mandato de supervisión de Red en Anillo 226
 - mandato de supervisión de Red en Anillo
 - Rápida 235
 - mandatos de configuración de Red en Anillo 222, 226
 - mandatos de configuración de Red en Anillo
 - Rápida 232, 235
 - mandatos de configuración Frame Relay 591
 - mandatos de configuración PPP 649
 - mandatos de supervisión Frame Relay 613
 - mandatos de supervisión PPP 686

M

- mandato
 - exit 11
- mandato de supervisión ATM LLC
 - list 328
- mandato exit 11
- mandato perf 214
- mandatos
 - entrada 9
- mandatos Boot CONFIG
 - timeload 61
- mandatos CONFIG
 - add 77
 - boot 84
 - clear 91
 - change 84
 - delete 93
 - disable 94
 - disable-completion 94
 - enable 95
 - Enable-completion 95
 - event 96
 - features 96
 - List 97
 - load 101
 - network 102
 - patch 102
 - protocol 105
 - qconfig 106
 - recuperación del sistema 112
 - resumen de 76
 - set 106
 - system view 113
 - time 114
 - unpatch 115
 - update 115
 - write 115

- mandatos de configuración
 - establecer nivel de indicador
 - añadir prefijo a nombre de sistema principal 110
 - indicador GWCON 22
 - multilink PPP protocol (mp) 697
- mandatos de configuración ATM
 - acceso 315
 - add 317
 - disable 322
 - enable 321
 - interface 316
 - LE-Client 315
 - LE-Services 315
 - list 317
 - qos 317
 - remove 318
 - resumen 315
 - set 318
- mandatos de configuración de circuitos de marcación
 - delete 798
 - encapsulator 798
 - list 799
 - resumen de 797
 - set 801
- mandatos de configuración de Ethernet 10/100
 - acceso 285
- mandatos de configuración de Ethernet de 10/100 Mbps
 - exit 288
- mandatos de configuración de filtros de red ELS
 - create 174
 - delete 175
 - disable 175
 - enable 175
 - list 176
 - visión general 173
- mandatos de configuración de Interfaz virtual ATM
 - add 323
 - list 323
 - remove 323
 - resumen 322
- mandatos de configuración de la gestión de cambios
 - add 52
 - copy 52
 - describe 54
 - disable 55
 - enable 55
 - erase 56
 - list 57
 - lock 58
 - set 59
 - tftp 60
 - unlock 63
 - update-firmware 64
- mandatos de configuración de Red en Anillo
 - acceso 221
 - habilitación para LLC 224
 - list 221
 - llc 226
 - LLC 222
 - media 222
 - packet-size 223
- mandatos de configuración de Red en Anillo
 - (continuación)
 - resumen de 221
 - set 223
 - source-routing 224
 - speed 224
- mandatos de configuración de Red en Anillo Rápida
 - acceso 231
 - habilitación para LLC 234
 - list 232
 - LLC 232, 235
 - media 232
 - packet-size 232
 - resumen de 231
 - set 233
 - source-routing 233
 - speed 234
- mandatos de configuración del rendimiento
 - disable 214
 - enable 214
 - list 214
 - resumen 214
 - set 214
- mandatos de configuración ELS
 - add 158
 - advanced 158
 - almacenamiento intermedio de mensajes 176
 - list 176
 - log 177
 - nolog 177
 - set 178
 - clear 158
 - default 159
 - delete 159
 - display 159
 - filter 160
 - list 160
 - nodisplay 162
 - noremove 162
 - notrace 164
 - notrap 164
 - remote 165
 - resumen de 157
 - set 167
 - trace 199
 - trap 173
- mandatos de configuración Ethernet
 - acceso 267
 - connector-Type 268
 - duplex 286
 - ip-encapsulation 268, 338
 - list 268
 - physical-address 268, 287
 - resumen 267, 285
- mandatos de configuración Ethernet de 10/100 Mbps
 - ip-encapsulation 286
 - list 287
- mandatos de configuración FDDI 243
 - acceso 243
 - list 243
 - set 244

- mandatos de configuración Frame Relay 572, 576
 - add 562
 - frame-handler-pvc 562
 - permanent-virtual-circuit 562
 - protocol-address 562
 - add-protocol
 - protocolo AppleTalk2 566
 - protocolo DN 566
 - protocolo IPX 566
 - add protocol-address
 - protocolo IP 566
 - change 571
 - disable
 - cir-monitor 572
 - cllm 572
 - compression 572
 - congestión 547
 - congestion-monitor 573
 - dn-length-field 573
 - encryption 573
 - fragmentation 573
 - lmi 573
 - lower-dtr 573
 - multicast-emulation 573
 - no-pvc 573
 - notify-fecn-source 573
 - orphan-circuits 573
 - point-to-point 573
 - protocol-broadcast 573
 - throttle-transmit-on-fecn 573
 - enable
 - cir-monitor 576
 - cllm 576
 - compression 576
 - congestión 547
 - congestion-monitor 576
 - dn-length-field 576, 578
 - encryption 576, 578
 - lmi 576
 - lower-dtr 576
 - multicast-emulation 576
 - no-pvc 576
 - notify-fecn-source 576
 - orphan-circuits 576
 - point-to-point 576
 - protocol-broadcast 576
 - throttle-transmit-on-fecn 576
 - list
 - all 583
 - fragmentation-capable-pvcs 583
 - frame-handler-pvc 583
 - hdlc 583
 - interfaz 583
 - lmi 583
 - permanent-virtual-circuits 583
 - protocol-address 583
 - pvc-groups 583
 - queues 602
 - subinterfaces 583
 - llc 591

- mandatos de configuración Frame Relay 572, 576
 - (continuación)
 - remove
 - frame-handler-pvc 592
 - permanent-virtual-circuit 592
 - protocol-address 592
 - remove-protocol
 - protocolo DN 593
 - remove protocol-address
 - protocolo Appletalk2 593
 - protocolo IP 592
 - protocolo IPX 592
 - resumen de 561
 - set
 - cable 594
 - clocking 594
 - crc-type 594
 - default cir 594
 - frame-size 594
 - lmi-type 594
 - n1-parameter 594
 - n2-parameter 594
 - n3-parameter 594
 - p1-parameter 594
 - parámetro transmit delay 594
 - redials 594
 - t1-parameter 594
 - t2 parameter 594
 - mandatos de configuración LLC
 - acceso 251
 - list 252, 351
 - resumen 251, 351, 363
 - set 252, 351
 - mandatos de configuración Point-to-Point
 - acceso 639
 - list 644
 - LLC 649
 - resumen de 640
 - mandatos de configuración PPP
 - establecimiento de parámetros IPCP 649
 - establecimiento de parámetros LCP 649
 - list
 - ccp 645
 - ecp 645
 - set 649
 - mandatos de configuración RDSI
 - establecer variante de conmutador 787
 - list 784
 - remove 784
 - resumen de 783
 - set 784
 - mandatos de configuración SDLC
 - add 726
 - delete 728
 - disable 728
 - enable 728, 741
 - list 729
 - msgsz 744
 - resumen de 726
 - set 732

- mandatos de configuración SDLC Relay
 - add 710
 - delete 712
 - disable 712
 - enable 712
 - list 713, 714
 - resumen de 710
 - set 715
- mandatos de configuración V.25bis
 - list 756
 - resumen de 755
 - set 757
- mandatos de configuración X.25
 - add 485
 - change 492
 - delete 493
 - disable 476
 - enable 475
 - list 494
 - national disable 479
 - national enable 476
 - national restore 484
 - national set 479
 - resumen de 469
 - set 470
- mandatos de supervisión
 - LAN Emulation Client (LEC) 333
 - multilink ppp protocol (mp) 701
- mandatos de supervisión ATM
 - acceso 323
 - atm-llc 324
 - interface 324, 325, 327
 - list 325
 - resumen 324
 - trace 326
 - wrap 327
- mandatos de supervisión de circuito de marcación
 - callback 804
- mandatos de supervisión de Ethernet de 10/100 Mbps
 - collisions 289
- mandatos de supervisión de filtros de red ELS
 - create 204
 - delete 205
 - disable 205
 - enable 206
 - list 206
 - visión general 204
- mandatos de supervisión de interfaces
 - adaptador de canal 431
 - LCS 436
 - LSA 438
 - MPC+ 441
- mandatos de supervisión de interfaz virtual ATM
 - resumen 328
- mandatos de supervisión de la Red en Anillo Rápida
 - dump 234
 - resumen de 234
- mandatos de supervisión de Red en Anillo
 - acceso 224, 234
 - dump 225
- mandatos de supervisión de Red en Anillo
 - (continuación)
 - resumen de 225
- mandatos de supervisión del rastreo de paquetes
 - off 202
 - on 202
 - packet Trace 188
 - reset 202
 - set 202
 - subsystems 203
 - trace-status 203
 - view 204
- mandatos de supervisión del rendimiento
 - acceso 215
 - disable 215
 - enable 215
 - list 216
 - report 216
 - resumen de 215
 - set 216
- mandatos de supervisión ELS
 - advanced 181
 - almacenamiento intermedio de mensajes 206
 - flush 207
 - list 207
 - log 207
 - nolog 208
 - read-file 209
 - set 209
 - tftp 210
 - view 211
 - write-buffer 212
 - clear 181
 - display 182
 - files 182
 - filter 183
 - list 183
 - nodisplay 185
 - noremote 186
 - notrace 187
 - notrap 187
 - remote 188
 - remove 190
 - restore 191
 - resumen 180
 - retrieve 191
 - save 191
 - set 191
 - statistics 197
 - trap 200
 - view 201
- mandatos de supervisión Ethernet 270
 - collisions 270
 - resumen 269
- mandatos de supervisión Ethernet de 10/100 Mbps
 - acceso 288
 - resumen 289
- mandatos de supervisión FDDI
 - acceso 246
 - list 246
 - SRT-STATS 246

- mandatos de supervisión Frame Relay
 - clear 600
 - disable 601
 - cllm 601
 - notify-fecn-source 601
 - throttle-transmit-on-fecn 601
 - enable 601
 - cllm 601
 - notify-fecn-source 601
 - throttle-transmit-on-fecn 601
 - list 601
 - all 601
 - circuito 601
 - frame-handler-pvc 601
 - interface 601
 - lmi 601
 - permanent-virtual-circuits 601
 - pvc-groups 602
 - subinterfaces 602
 - llc 613
 - notrace 613
 - resumen de 600
 - set 613
 - trace 615
- mandatos de supervisión IP
 - ping 38
- mandatos de supervisión LEC
 - acceso 353
 - list 354
 - mib 358
 - resumen de 353
- mandatos de supervisión LLC
 - acceso 254
 - clear-counters 255
 - list 255, 363
 - resumen 255
 - set 261, 363
- mandatos de supervisión multilink PPP protocol (mp)
 - acceso 701
- mandatos de supervisión PPP
 - clear 662
 - list 662
 - dn 684
 - dncp 684
 - osi 685
 - osicp 685
 - listado de parámetros IPCP 662
 - listado de parámetros LCP 662
 - llc 686
 - resumen de 662
- mandatos de supervisión RDSI
 - calls 790
 - circuits 790
 - channels 790
 - L2_Counters 792
 - L3_Counters 792
 - parameters 792
 - resumen de 789
 - statistics 793
 - TEI 792
- mandatos de supervisión SDLC
 - acceso 739
 - clear 740
 - link counters 741
 - list 741
 - resumen de 739
- mandatos de supervisión SDLC Relay
 - clear-port-statistics 718
 - disable 718
 - enable 719
 - list 719
 - resumen de 718
- mandatos de supervisión V.25bis
 - calls 760
 - circuits 761
 - parameters 762
 - resumen de 760
 - statistics 763
- mandatos de supervisión X.25
 - list 498
 - parameters 498
 - reset 499
 - resumen de 497
 - statistics 500
- mandatos GWCON
 - activate 118
 - buffer 119
 - clear 120
 - configuration 120
 - disable 123
 - disk 124
 - enable 124
 - error 125
 - event 126
 - features 126
 - interface 126, 219
 - memory 127
 - network 129
 - protocol 130
 - queue 130
 - reset 131
 - resumen de 118
 - statistics 132
 - test 132
 - uptime 133
- mandatos OPCON
 - configuration 34
 - console 34
 - diags 35
 - divert 35
 - els 36
 - event 36
 - flush 36
 - halt 37
 - intercept 37
 - logout 37
 - memory 38
 - reload 39
 - resumen de 33
 - status 40
 - suspend 41

- mandatos OPCON (*continuación*)
 - talk 41
 - telnet 42
- mandatos operativos Ethernet
 - acceso 269
- media
 - mandato de configuración de Red en Anillo 222
 - mandato de configuración de Red en Anillo Rápida 232
- memoria
 - borrado de información 190
- memoria de configuración no volátil
 - sustitución 84
- memory
 - mandato GWCON 127
 - mandato OPCON 38
 - obtención de información acerca 38
 - visualización de información acerca de 127
- mensajes
 - explicación 140
 - interpretación 139
 - recepción 135
- mensajes de rastreo de paquetes
 - rastreo de paquetes 188
- mensajes ELS 140
 - detección 173, 200
 - explicación 140
 - gestión de la rotación 142
 - grupos 141
 - habilitación de la anotación cronológica en un archivo remoto (Remote) 165, 188
 - información de red 141
 - nivel de anotación cronológica 139
 - rastreo 199
 - supresión de detección de (notrap) 187
 - supresión de detecciones 164, 187
 - supresión de la anotación cronológica remota (noremote) 162, 186
 - supresión de la visualización de 162
 - supresión de la visualización de (nodisplay) 185
 - supresión de rastreo 187
 - trace 172
- mib
 - mandato de supervisión del LEC 358
- mod, mandato de configuración de adaptador de canal 426
- modalidad de Configuración rápida 70
 - entrada manual 70
- modalidad de Sólo configuración
 - descripción 67
 - entrada automática 68
 - entrada manual 68
- Módem
 - inhabilitación 94, 95
- MP de múltiples chasis 693
 - configuración 695
- MS-CHAP
 - autenticación para PPP 629
- msgsz
 - mandato de supervisión SDLC 744

- multilink PPP protocol (MP)
 - configuración
 - circuitos de marcación 693
 - enlaces serie 694
 - MP de múltiples chasis 695
 - redes con túneles de capa 2 694
 - consideraciones 692
 - mandatos de configuración 697
 - mandatos de supervisión 701
 - múltiples chasis 693
 - relación con el túnel de capa 2 693
 - visión general 691
- MVS/ESA
 - definición de configuración de hardware 373
 - definición del 2216 en 373
 - HCD 373
- MVS/XA, definición del 2216 en 373

N

- national disable
 - mandato de configuración X.25 479
- national enable
 - mandato de configuración X.25 476
- national restore
 - mandato de configuración X.25 484
- national set
 - mandato de configuración X.25 479
- Negociación automática en la interfaz Ethernet de 10/100 Mbps 281
- net, mandato de supervisión de interfaces de canal 434
- network
 - entorno 102
 - environment 129
 - mandato 410
 - mandato CONFIG 102
 - mandato GWCON 129
- network, mandato 18, 267, 285, 315, 353, 639, 755
- Network Control Protocol (NCP)
 - para interfaces PPP 633
 - AppleTalk Control Protocol 633
 - APPN HPR Control Protocol 636
 - APPN ISR Control Protocol 636
 - Banyan VINES Control Protocol (BVCP) 633
 - Bridging Control Protocol (BCP) 633
 - Callback Control Protocol (CBCP) 634
 - DECnet Control Protocol (DNCP) 634
 - IP Control Protocol (IPCP) 634
 - IPv6 Control Protocol (IPv6CP) 635
 - IPX Control Protocol (IPXCP) 635
 - OSI Control Protocol (OSICP) 636
- nivel de indicador
 - funciones adicionales de
 - visualizar nombre de sistema principal con cambios 110
 - visualizar nombre de sistema principal con fecha 110
 - visualizar nombre de sistema principal con hora 110
 - visualizar nombre de sistema principal con retorno de carro 110

- nivel de indicador (*continuación*)
 - visualizar nombre de sistema principal con VPD 110
 - mandato de configuración
 - añadir prefijo a nombre de sistema principal 110
 - visualizar nombre de sistema principal 110
- nodisplay
 - mandato de configuración ELS 162
 - mandato de supervisión ELS 185
- noremote
 - mandato de configuración ELS 162
 - mandato de supervisión ELS 186
- Notificación explícita de congestión hacia adelante (FECN)
 - Frame Relay 539
- Notificación explícita de congestión hacia atrás (BECN)
 - Frame Relay 539
- Notificación y evitación de la congestión
 - Evitación explícita de congestión hacia adelante 547
 - Evitación explícita de congestión hacia atrás 547
- notrace
 - mandato de configuración ELS 164
 - mandato de supervisión ELS 187
 - mandatos de supervisión Frame Relay 613
- notrap
 - mandato de configuración ELS 164
 - mandato de supervisión ELS 187
- números de interfaz, visualización 431

O

- obtención de ayuda 11
- obtención de estado de sesión telnet 43
- off
 - mandato de supervisión del rastreo de paquetes 202
- on
 - mandato de supervisión del rastreo de paquetes 202
- opciones MPPE
 - listado 645
- OPCON
 - acceso a la interfaz de canal 409
 - interfaz de adaptador de canal, consola 431
- OSI Control Protocol (OSICP)
 - para PPP 636
- OSPF 814

P

- packet-size
 - mandato de configuración de Red en Anillo 223
 - mandato de configuración de Red en Anillo Rápida 232
- packet trace
 - mandato de supervisión del rastreo de paquetes 188
- palabras clave 828
- parameters
 - mandato de supervisión RDSI 792
 - mandato de supervisión X.25 498

- parameters (*continuación*)
 - mandatos de supervisión V.25bis 762
- parámetro de arranque para VTAM, ATCSTRxx 386
- parámetro de nombre de grupo 141
- parámetro de número de suceso 139
- parámetro pin
 - valor 167
- parámetros
 - configuración 106
 - emulación de LAN clave 291
 - número de suceso 139
 - para LAN Emulation 309
- parámetros clave para LAN Emulation 309
- paso a través TCP/IP
 - configuración 392
- patch
 - mandato CONFIG 102
- PCA
 - configuración 409
 - ejemplo de definición IOCP 371
 - visión general 388
- personalidad nacional, establecimiento 513
- physical-address
 - mandato de configuración Ethernet 268, 287
- ping
 - mandato de supervisión IP 38
- planificación y preparación
 - adaptador ESCON de 2216 387
 - sistema principal 367, 387
- Point-to-Point--consulte PPP 689
- Point-to-Point Protocol (PPP) 634
 - acceso al proceso de configuración 639
 - AppleTalk Control Protocol 633
 - APPN HPR Control Protocol 636
 - APPN ISR Control Protocol 636
 - autenticación 628
 - Banyan Vines Control Protocol (BVCP) 633
 - Bridging Control Protocol (BCP) 633
 - Callback Control Protocol (CBCP) 634
 - campo de control 623
 - campo de información 623
 - campo de protocolo 623
 - campo de secuencia de comprobación de tramas 623
 - campos de dirección 623
 - campos de distintivos 623
 - DECnet Control Protocol (DNCP) 634
 - estructura de trama 622
 - IPv6 Control Protocol (IPv6CP) 635
 - IPX Control Protocol (IPXCP) 635
 - Link Control Protocol (LCP) 624
 - Network Control Protocol (NCP) 633
 - OSI Control Protocol (OSICP) 636
 - paquetes de establecimiento de enlace 626
 - paquetes de mantenimiento de enlace 628
 - paquetes de terminación de enlace 627
 - paquetes LCP 625
 - visión general 621
- política de descriptor de rutas 297
- política de destino LAN (política de dirección MAC) 298

- política de dirección MAC (política de destino LAN) 298
- política de nombre de ELAN 298
- política de tamaño máximo de trama 297, 299
- política de tipo de ELAN 299
- políticas 291
 - acuerdo de 297
- políticas y valores de políticas 297
- PPP
 - IP Control Protocol (IPCP) 634
- primera
 - configuración 11
- proceso
 - segundo nivel
 - acceso 14
 - tercer nivel
 - acceso 16
- proceso CONFIG
 - acceso 14
 - descripción de 67
 - entrada 14, 76
 - mandatos disponibles desde 76
 - salida 76
 - vuelcos del sistema 75
- proceso de consola, acceso 431
- proceso de consola de protocolo
 - entrada 22
- proceso de gestión de mensajes
 - descripción de 135
 - entrada y salida 135
 - mandatos OPCON 135
 - mandatos que afectan 135
 - recepción de mensajes 135
- proceso de supervisión de interfaces PPP
 - acceso 661
- proceso GWCON
 - descripción de 117
 - entrada y salida 117
- proceso MONITR
 - descripción de 135
 - entrada y salida 135
 - mandatos OPCON 135
 - mandatos que afectan 135
 - recepción de mensajes 135
- proceso OPCON
 - acceso 33
 - descripción 33
 - mandatos disponibles en 33
 - resumen 6
 - volver a 11
- procesos
 - comunicación con 6
 - lista de 6
- procesos de dispositivo
 - conexión a 9, 41
 - visualización de información acerca de 40
- programa de definición de la configuración de hardware 367
- protocol
 - mandato CONFIG 105
 - mandato GWCON 130

- protocol, mandato 22, 23
- protocolo
 - entrada en el proceso de configuración 22
 - proceso de configuración 219, 220
 - proceso de consola 219, 220
- protocolos
 - configuración utilizando la configuración rápida 812
 - entrada en el entorno de configuración para 105
 - entrada en proceso de consola 22
 - generación de una lista de 105
 - proceso de consola 15
 - procesos de configuración y consola
 - acceso 22
 - visualización de información acerca de 120
- pvc de manejador de tramas Frame Relay
 - cambio 572
- PVC manejadores de tramas
 - Frame Relay 534

Q

- qconfig
 - mandato CONFIG 106
- QoS
 - mandato de configuración ATM 317
- queue
 - mandato GWCON 130

R

- radius 827
- RDSI
 - acceso al proceso de supervisión 789
 - circuitos de marcación 770
 - configuración 777, 783
 - configuración de PPP 776
 - configuraciones de ejemplo 774
 - conmutadores soportados 776
 - contención de circuitos de marcación 771
 - control del coste a través de circuitos a petición 771
 - delete address 93
 - direcciones 771
 - mandatos GWCON 793
 - reconfiguración dinámica 795
 - requisitos y restricciones 776
 - restricciones de interfaz 776
 - verificación de la llamada 772
 - visión general 769
- reconfiguración 388
- reconfiguración dinámica
 - canal de bucle de retorno APPN 457
 - canal ESCON 447
 - canal LCS 453
 - canal LSA 451
 - canal MPC 455
 - canal PCA 449
 - ethernet 270
 - frame relay 617
 - interfaz ATM 328
 - interfaz de red ethernet de 10/100 Mbps 289

- reconfiguración dinámica (*continuación*)
 - LEC 364
 - PPP 689
 - RDSI 795
 - red en anillo 229
 - Relay de SDLC 720
 - X.25 504
 - XTP 530
- reconfiguración dinámica de ethernet 270
- reconfiguración dinámica de frame relay 617
- reconfiguración dinámica de interfaz ATM 328
- reconfiguración dinámica de la interfaz de red ethernet de 10/100 Mbps 289
- reconfiguración dinámica de LEC 364
- reconfiguración dinámica de PPP 689
- reconfiguración dinámica de red en anillo 229
- reconfiguración dinámica de SDLC Relay 720
- reconfiguración dinámica de X.25 504
- reconfiguración dinámica XTP 530
- recuperación del sistema
 - mandato CONFIG 112
- red en anillo
 - tipos de encapsulación para IPX 815
- Red en Anillo Rápida
 - configuración 231
- redes con túneles de capa 2
 - configuración para MP 694
- redundancia de servidores de LAN Emulation 306
- reenviador de paquetes
 - entrada en el entorno CONFIG para 105
- registro de direcciones en LAN Emulation 301
- reload
 - mandato OPCON 6, 39
- Reload
 - mandato OPCON 15
- reloj, establecimiento y cambio 114
- remote
 - mandato de configuración ELS 165
 - mandato de supervisión ELS 188
- remove
 - mandato de configuración ATM 318
 - mandato de configuración de Interfaz virtual ATM 323
 - mandato de configuración Frame Relay 592
 - mandato de configuración RDSI 784
 - mandato de supervisión ELS 190
- rendimiento
 - configuración 213
- report
 - mandato de supervisión del rendimiento 216
- reset
 - mandato de supervisión del rastreo de paquetes 202
 - mandato de supervisión X.25 499
 - mandato GWCON 131
- resolución de direcciones en la LAN Emulation 301
- restore
 - mandato de supervisión ELS 191
- retrieve
 - mandato de supervisión ELS 191
- RIP 814

S

- salida
 - eliminación 36
 - envío a otras consolas 35
 - suspensión 37
- salir
 - entornos de nivel inferior 11
- salir del dispositivo 6
- save
 - mandatos de supervisión ELS 191
- SDLC
 - acceso a la configuración 725
 - configuración 723, 725
 - interfaz de llamada de entrada conmutada configuración 723
 - interfaz de red 749
 - procedimiento de configuración 723
 - requisitos de configuración 724
- SDLC Relay
 - acceso a la configuración 709
 - acceso al entorno de supervisión 717
 - configuración 707, 709
- segundo nivel
 - proceso
 - acceso 14
- seguridad de LAN Emulation 308
- selector 293
- sesión
 - terminación 38
- set
 - adaptador de canal
 - mandato de configuración 430
 - mandato CONFIG 106
 - mandato de configuración ATM 318
 - mandato de configuración de circuito de marcación 801
 - mandato de configuración de la gestión de cambios 59
 - mandato de configuración de Red en Anillo 223
 - mandato de configuración de Red en Anillo Rápida 233
 - mandato de configuración del rendimiento 214
 - mandato de configuración ELS 167
 - mandato de configuración Frame Relay 593
 - mandato de configuración LLC 351
 - mandato de configuración PPP 649
 - mandato de configuración SDLC 732
 - mandato de configuración SDLC Relay 715
 - mandato de configuración V.25bis 757
 - mandato de configuración X.25 470
 - mandato de configuración XTP 524
 - mandato de supervisión del rastreo de paquetes 202
 - mandato de supervisión del rendimiento 216
 - mandato de supervisión ELS 191
 - mandato de supervisión Frame Relay 613
 - mandato de supervisión LLC 261, 363
 - mandato de supervisión SDLC 744
 - mandatos de configuración RDSI 784
- sistema operativo
 - definición del 2216 en 372

- sistema principal
 - bloques de control 381
 - conexión del 2216, actividades necesarias 367
 - programa de configuración de la entrada/salida 367
 - programas
 - VTAM, configuración 385, 386
- sistema principal MVS, configuración para TCP/IP 374
- software
 - interfaz de usuario 6
 - visión general 6
- software de direccionador
 - comunicación con 130
- software de dispositivo
 - interfaz de usuario 3
 - volver a cargar 39
- software de red
 - visualización de información de estadísticas acerca de 132
- soporte CLLM 548
- source-routing
 - mandato de configuración de Red en Anillo Rápida 224
 - mandato de configuración de Red en Anillo Rápida 233
- speed
 - mandato de configuración de Red en Anillo Rápida 224
 - mandato de configuración de Red en Anillo Rápida 234
- statistics
 - mandato de supervisión ELS 197
 - mandato de supervisión RDSI 793
 - mandato de supervisión X.25 500
 - mandato GWCON 132
 - mandatos de supervisión V.25bis 763
- status
 - mandato OPCON 40, 639
- subcanales
 - LCS, configuración 412
 - LSA, configuración 416
 - MPC+, configuración 420
 - número proporcionado 388
- subinterfaces
 - Frame Relay 533
- subsystems
 - mandato de supervisión del rastreo de paquetes 203
- Sucesos
 - Causas 138
- sugerencias
 - configuración 11
- supervisión
 - acceso a los mandatos mp 701
 - ATM 315
 - indicador, visualización 431
 - interfaces de red 21
 - mandatos de supervisión del rendimiento 215
- Supervisión de la congestión 547
- supresión de información de configuración 91
- suspend
 - mandatos OPCON 41
- system view
 - mandato CONFIG 113

T

- TACACS 831
- talk
 - mandato OPCON 41, 213, 215
- Tamaño de exceso de ráfaga
 - definición 544
 - establecimiento para Frame Relay 544
- Tamaño de ráfaga confirmado
 - definición 544
 - relación con el tamaño máximo de trama 544
- TCP/IP
 - configuración de Estación de canal LAN (LCS) 374
 - configuración del canal de diversas vías de acceso+ (MPC+) 376
 - configuración del sistema principal MVS 374
 - definición del 2216 para MVS o VM para el LCS, ejemplo 377
 - definición del 2216 para MVS o VM para MPC+, ejemplo 379
- TCP/IP, transporte de tráfico X.25 a través de TDM (multiplexación de la división de tiempo) 505
- TEI
 - mandato de supervisión RDSI 792
- telnet
 - cierre de una conexión 43
 - mandato OPCON 42
 - obtención de estado de sesión Telnet 43
 - salir de una sesión 43
- telnet, mandato 42
- temporizador de mantener activo, establecimiento para XTP 524
- temporizador de petición de conexión 509
- tercer nivel
 - proceso
 - acceso 16
- terminales locales 3
- terminales remotos 4
- test
 - mandato GWCON 132
 - mandatos de supervisión SDLC 748
 - test 748
- tftp
 - mandato de configuración de la gestión de cambios 60
- TFTP
 - descripción de
 - relacionada con la gestión de cambios 47
- time
 - mandato CONFIG 114
- timeload
 - mandato Boot CONFIG 61
- Tinygram compression 650
- tipo de cable, cronometraje y 459
- tipo de encapsulación 816
- TLV
 - definidos en una ELAN 300
- trace
 - mandatos de configuración ELS 199
 - mandatos de supervisión ATM 326
 - mandatos de supervisión Frame Relay 615

- trace, mandato de supervisión de interfaces de canal 435
- trace-status
 - mandato de supervisión del rastreo de paquetes 203
- trap
 - mandato de supervisión ELS 200
 - mandatos de configuración ELS 173
- tune
 - mandato de supervisión de interfaces LCS 438
 - mandato de supervisión de interfaces MPC+ 446
 - mandato de supervisión de interfaz LSA 440
- tune, mandato de supervisión de interfaces de canal 435
- túnel de capa 2
 - relación con multilink PPP (MP) 693

U

- UNIX
 - desensamblaje de un archivo de carga 825
 - ensamblaje de un archivo de carga 823
- unlock
 - mandato de configuración de la gestión de cambios 63
- unpatch
 - mandato CONFIG 115
- update
 - mandato CONFIG 115
- update-firmware
 - mandato de configuración de la gestión de cambios 64
- uptime
 - mandato GWCON 133

V

- V.25bis
 - acceso a la configuración 755
 - acceso al proceso de supervisión 759
 - adición de direcciones 751
 - configuración 751, 755
 - mandatos GWCON 764
- V25 bis address 101
- valores de longitud de tipo 300
- valores de política de duplicados 299
- valores por omisión de los parámetros X.25 462
- variante de conmutador 781
 - establecimiento para RDSI 787
- variante de conmutador I.431 781
- VC
 - Frame Relay 531
- VCC de datos directos 303
- Velocidad de información de circuito (CIR) 543
- Velocidad de línea 545
- velocidad máxima de información
 - para frame relay 545
- velocidad mínima de información
 - para frame relay 545

- velocidad variable de información
 - para frame relay 545
- verificación de la llamada RDSI 772
- view
 - mandato de supervisión del rastreo de paquetes 204
 - mandato de supervisión ELS 201
- virtual
 - interfaz
 - LCS, configuración 411
 - LSA, configuración 414
 - MPC+, configuración 418
 - manejadores de red 388
- visión general
 - conexiones virtuales (VC) 636
 - de software 6
 - mandatos de configuración de filtros de red ELS 173
 - mandatos de supervisión de filtros de red ELS 204
- visión general de FDDI 239
- visión general de LAN Emulation 291
- visión general del adaptador de canal 388
- visualización
 - base de datos de configuración de arranque 57
 - visualización del indicador de supervisión 431
 - visualizar nombre de sistema principal 110
 - visualizar nombre de sistema principal con cambios 110
 - visualizar nombre de sistema principal con fecha 110
 - visualizar nombre de sistema principal con hora 110
 - visualizar nombre de sistema principal con retorno de carro 110
 - visualizar VPD del software del nombre de sistema principal 110
- VM/ESA, definición del 2216 en 372
- VM/SP, definición del 2216 en 372
- VM/XA, definición del 2216 en 372
- volver a cargar 15
 - dispositivo 6
- volver a cargar el dispositivo 819
- VSE/ESA, definición de 2216 373
- VTAM
 - archivo de inicialización ATCSTRxx 386
 - conexión LSA directa, configuración 382
 - configuración del sistema principal
 - conexión APPN, LSA 382
 - conexión DLSw 383
 - MPC+ 385, 386
 - parámetro de arranque 386
- vuelcos del sistema, utilización 75

W

- wrap
 - mandatos de supervisión ATM 327
- write
 - mandato CONFIG 115

X

X.25

valores por omisión de los parámetros 462

X.25 Transport Protocol (XTP) 505

XTP

configuración 519

establecimiento de personalidad nacional 513

establecimiento del temporizador de mantener
activo 524

función de similar de reserva 508

grupos de usuarios cerrados
visión general 509

mandatos de configuración 519

Add 519

Change 522

Delete 522

Disable 524

Enable 524

List 524

Set 524

mandatos de supervisión

Add 526

Delete 527

List 527

procedimientos de configuración 510

utilización 505

XTP local

descripción 509

XTP local

descripción 509

Hoja de Comentarios

Nways Multiprotocol Access Services
Guía del usuario de software
Versión 3.4

Número de Publicación SC10-3434-01

Por favor, sírvase facilitarnos su opinión sobre esta publicación, tanto a nivel general (organización, contenido, utilidad, facilidad de lectura,...) como a nivel específico (errores u omisiones concretos). Tenga en cuenta que los comentarios que nos envíe deben estar relacionados exclusivamente con la información contenida en este manual y a la forma de presentación de ésta.

Para realizar consultas técnicas o solicitar información acerca de productos y precios, por favor diríjase a su sucursal de IBM, business partner de IBM o concesionario autorizado.

Para preguntas de tipo general, llame a "IBM Responde" (número de teléfono 901 300 000).

Al enviar comentarios a IBM, se garantiza a IBM el derecho no exclusivo de utilizar o distribuir dichos comentarios en la forma que considere apropiada sin incurrir por ello en ninguna obligación con el remitente.

Comentarios:

Gracias por su colaboración.

Para enviar sus comentarios:

- Envíelos por correo a la dirección indicada en el reverso.
- Envíelos por correo electrónico a: <http://www.networking.ibm.com/feedback/pubsurv.html>

Si desea obtener respuesta de IBM, rellene la información siguiente:

Nombre

Dirección

Compañía

Número de teléfono

Dirección de e-mail

IBM S.A.
National Language Solutions Center
Av. Diagonal, 571
08029 - Barcelona



SC10-3434-01



Spine information:



Nways Multiprotocol Access
Services

MAS V3.4 Guía del usuario de software