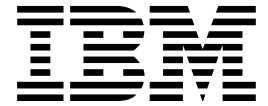
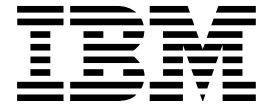


Nways Multiprotocol Routing Services



Manual de consulta de supervisión y configuración de protocolos Volumen 2 Versión 3.4

Nways Multiprotocol Routing Services



Manual de consulta de supervisión y configuración de protocolos Volumen 2 Versión 3.4

Nota

Antes de usar el presente documento, lea la información general que se encuentra bajo "Avisos" en la página xix.

Segunda edición (Octubre 1999)

Esta publicación es la traducción del original inglés *Nways Multiprotocol Routing Services Protocol Configuration and Monitoring Reference Volume 2 Version 3.4* (SC30-3865-06).

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

Solicite las publicaciones al representante de IBM o a la sucursal de IBM que le atiende localmente. Las publicaciones no se almacenan en la dirección indicada más abajo.

IBM estará agradecida por los comentarios que le envíen. En la parte posterior de esta publicación, se proporciona un formulario para los comentarios del lector. Si se ha extraído el formulario, puede enviar los comentarios a:

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

Cuando envíe información a IBM, estará dando permiso, no exclusivo, a esta compañía para que use o distribuya la información de la forma que considere más apropiada, sin incurrir por ello en ninguna obligación hacia el informante.

Contenido

Avisos	xix
Marcas registradas	xxi
Prefacio	xxiii
Quién debe leer este manual	xxiii
Obtención de información adicional	xxiii
Acerca del software	xxiii
Convenios utilizados en este manual	xxiv
Publicaciones de IBM 2210 Nways Multiprotocol Router	xxv
Resumen de los cambios para la biblioteca de software de IBM 2210	xxvi
Cómo obtener ayuda	xxix
Cómo salir de un entorno de nivel inferior	xxix
Uso de APPN	1
¿Qué es APPN?	1
Comunicaciones de igual a igual	1
Tipos de nodos APPN	1
¿Qué funciones de APPN se implementan en el direccionador?	4
Características opcionales del nodo de red APPN	7
Direccionamiento de alto rendimiento	8
Peticiónario de LU dependientes (DLUR)	10
Redes de conexiones APPN	14
Branch Extender	16
Extended Border Nodes	17
Comparación de Branch Extender con Extended Border Node	19
Gestión de un nodo de red	20
Posibilidades del punto de entrada para alertas relacionadas con APPN	20
Posibilidades SNMP para las MIB de APPN	22
Recogida de desechos (Garbage Collection) de la base de datos de topología	22
Cola de alertas retenidas configurable	22
Punto focal implícito	23
Soporte de Enterprise Extender para HPR sobre IP	23
DLC con soporte	23
Proceso de configuración del direccionador	24
Cambios en la configuración que necesitan un reinicio de la función APPN	24
Requisitos de configuración de APPN	25
Configuración del direccionador como nodo de red de APPN	25
Configuración de Branch Extender	29
Configuración de Extended Border Nodes	30
Direccionamiento de alto rendimiento	36
DLUR	36
Configuración de los puntos focales	37
Configuración del tamaño de la cola de retención de alertas	37
Definición de las características de los grupos de transmisión (TG)	37
Calculo de rutas de APPN usando las características de los TG	38
Opciones de CoS	39
Ajuste del nodo APPN	40
Servicio de nodo (Rastreo)	41

Estadísticas de nodo y de contabilidad	41
Algoritmo de reintento del DLUR	42
Implementación de APPN en el direccionador usando DLSw	45
Implementación de la red de conexiones APPN Frame Relay BAN	46
Listas de parámetros del nivel de puerto	50
Listas de parámetros del nivel de enlace	50
Lista de parámetros de LU	51
Listas de parámetros del nivel de nodo	51
Notas sobre la configuración de APPN	51
Configuración de un circuito permanente usando RDSI	51
Configuración de APPN sobre circuitos de marcación bajo pedido	54
Configuración del redireccionamiento de la WAN	58
Configuración de la restauración de la WAN	65
Configuración de V.25 bis	67
Configuración de V.34	68
Configuración de APPN sobre ATM	71
Configuración de APPN usando SDLC	73
Configuración de APPN sobre X.25	80
Configuración de APPN sobre Frame Relay	84
Configuración de APPN sobre Frame Relay BAN	85
Configuración del soporte de Enterprise Extender para HPR sobre IP	86
Configuración de redes de conexiones sobre HPR sobre IP	87
Configuración de un Extended Border Node	87
Uso de TN3270	89
Visión general	89
Ubicación de la función de servidor de TN3270	90
Función de servidor de TN3270E	90
Guardado en antememoria de clientes de Host On-Demand de TN3270	93
Configuración general del servidor de TN3270E	94
Carga del código de servidor de TN3270	94
Configuración de TN3270 bajo el protocolo APPN	94
Dirección IP del servidor	94
Puertos TCP del servidor	95
Definición de las PU	96
Definición de las LU	97
LU configuradas	98
Definición dinámica de LU dependientes (DDDLU)	99
Definición dinámica iniciada por un sistema principal de LU dependientes (HIDLU)	101
Correlación de clientes con LU	102
Correlación de direcciones IP de cliente con LU/grupaciones	104
Asociación del puerto TCP del servidor con una agrupación	107
Combinación de la correlación de dirección IP y puerto	108
Equilibrio de carga entre varias PU	108
Configuraciones de ejemplo	109
Configuración de TN3270 mediante DLUR	109
Configuración de TN3270E usando una conexión de subárea	112
Otras configuraciones de ejemplo	114
Configuración y supervisión de APPN	117
Acceso al proceso de configuración de APPN	117
Resumen de los mandatos de configuración de APPN	117
Información detallada sobre los mandatos de configuración de APPN	119

Enable/Disable	119
Set	119
Add	154
Delete	217
List	217
Activate_new_config	217
TN3270E	218
Supervisión de APPN	230
Acceso a los mandatos de supervisión de APPN	230
Mandatos de supervisión de APPN	231
Detalles de los mandatos de supervisión de APPN	235
Mandatos de supervisión de TN3270E	271
Deactivate LU	272
List	272
Soporte de reconfiguración dinámica de APPN	283
Delete Interface de CONFIG (Talk 6)(Suprimir interfaz)	283
Activate Interface de GWCON (Talk 5)(Activar interfaz)	283
Reset Interface de GWCON (Talk 5)(Restablecer interfaz)	283
Mandatos Component Reset de GWCON (Talk 5)(Restablecer componente)	284
Mandatos Activate de CONFIG (Talk 6)(Activar)	284
Uso de AppleTalk Phase 2	285
Procedimientos de configuración básicos	285
Habilitación de parámetros del direccionador	285
Establecimiento de los parámetros de red	286
AppleTalk sobre PPP	286
Filtros de zona de AppleTalk 2	287
Información general	287
¿Para qué sirven los filtros de nombre de zona?	287
¿Cómo se añaden filtros?	288
Ejemplos de procedimientos de configuración	288
Configuración y supervisión de AppleTalk Phase 2	293
Acceso al entorno de configuración de AppleTalk Phase 2	293
Mandatos de configuración de AppleTalk Phase 2	293
Add	294
Delete	295
Disable	296
Enable	297
List	299
Set	300
Acceso al entorno de supervisión de AppleTalk Phase 2	302
Mandatos de supervisión de AppleTalk Phase 2	302
Atecho	302
Cache	303
Clear Counters	304
Counters	304
Dump	304
Interface	305
Uso de VINES	307
Visión general de VINES	307
VINES sobre protocolos e interfaces de direccionador	307

Nodos cliente y de servicio	307
Protocolos de capa de red de VINES	308
VINES Internet Protocol (VINES IP)	308
Routing Update Protocol (RTP)	310
Internet Control Protocol (ICP)	313
VINES Address Resolution Protocol (VINES ARP)	314
Procedimientos de configuración básicos	315
Ejecución de Banyan VINES en el direccionador de puenteo	315
Ejecución de Banyan VINES sobre enlaces de WAN	315
Configuración y supervisión de VINES	317
Acceso al entorno de configuración de VINES	317
Mandatos de configuración de VINES	317
Add	317
Delete	318
Disable	318
Enable	319
List	319
Set	320
Acceso al entorno de supervisión de VINES	321
Mandatos de supervisión de VINES	321
Counters	322
Dump	323
Route	325
Uso de DNA IV	327
Visión general de DNA IV	327
Terminología y conceptos de DNA IV	328
Direccionamiento	329
Tablas de direccionamiento	330
Direccionadores de áreas	330
Configuración de los parámetros de direccionamiento	330
Implementación de DNA IV efectuada por IMB	331
Gestión de tráfico utilizando el control de acceso	332
Gestión del tráfico con filtros de direccionamiento de áreas	335
Configuración de DNA IV	340
Configuración y supervisión de DNA IV	345
Mandatos de configuración y supervisión de DNA IV	345
Define/Set	346
Purge	355
Set	356
Show	356
Show/List	359
Zero	365
Uso de OSI/DECnet V	367
Visión general de OSI	367
Direccionamiento de NSAP	368
IDP	369
DSP	369
Formato de direccionamiento IS-IS	369
NSAP de GOSIP Versión 2	370
Direcciones de difusión múltiple	370

Direccionamiento OSI	371
Protocolo IS-IS	371
Áreas IS-IS	372
Dominio IS-IS	372
Mensaje hello de IS a IS (IIH)	374
Mensaje L1 IIH	374
Mensaje L2 IIH	375
Mensaje IIH de punto a punto	375
IS designado	375
Bases de datos de estados de enlaces	376
Tablas de direccionamiento	377
Codificación de prefijos de direcciones	380
Contraseñas de autenticación	381
Protocolo ESIS	381
Mensaje hello	382
Mensaje hello de sistema final (ESH)	382
Mensajes hello de sistema intermedio (ISH)	382
Circuitos X.25 para DECnet V/OSI	382
Circuitos de direccionamiento	382
Filtros	383
Plantillas	383
Inicialización de enlaces	384
Configuración de OSI/DECnet V	384
Procedimiento de configuración básico	384
Configuración de OSI sobre una LAN Ethernet o red en anillo	385
Configuración de OSI sobre X.25 o Frame Relay	385
Configuración de un direccionador DNA V para un entorno DNA IV	385
Consideraciones de algoritmo de DNA IV y DNA V	386
Configuración y supervisión de OSI/DECnet V	387
Acceso al entorno de configuración de OSI	387
Mandatos de configuración de OSI/DECnet V	387
Add	388
Change	395
Clear	397
Delete	398
Disable	400
Enable	400
List	401
Set	408
Acceso al entorno de supervisión de OSI/DECnet V	415
Mandatos de supervisión de OSI/DECnet V	415
Addresses	416
Change Metric	416
CLNP-Stats	417
Designated-router	419
DNAV-info	419
ES-Adyacencias	420
ES-IS-Stats	420
IS-Adyacencias	423
IS-IS-Stats	423
L1-Routes	425
L2-Routes	425
L1-Summary	426

L2-Summary	427
L1-Update	427
L2-Update	428
Ping-1139	429
Route	429
Send (Echo Packet)	430
Subnets	430
Toggle (Alias/No Alias)	431
Traceroute	431
Uso de NHRP	433
Visión general de Next Hop Resolution Protocol (NHRP)	433
Beneficios de la implementación de IBM y NHRP	434
Características de rendimiento	435
Ejemplos de configuraciones de NHRP	436
Implementación de NHRP	440
Parámetros de configuración	442
Configuración y supervisión de NHRP	449
Acceso al proceso de configuración de NHRP	449
Mandatos de configuración de NHRP	449
Enable NHRP	450
Disable NHRP	450
Advanced Config	450
List	450
Mandatos de configuración avanzada de NHRP	451
Add	452
Delete	453
Change	454
List	455
Set	456
Acceso al proceso de supervisión de NHRP	460
Mandatos de supervisión de NHRP	460
Box Status	460
Interface Status	461
Statistics	461
Cache	462
Server_purge_cache	462
MIB	462
Métodos abreviados LANE	463
CONFIG Parameters	464
Reset	465
Rastreo de paquetes de NHRP	466
NHRP Soporte de reconfiguración dinámica del servidor NHRP	467
Delete Interface de CONFIG (Talk 6)(Suprimir interfaz)	467
Activate Interface de GWCON (Talk 5)(Activar interfaz)	467
Reset Interface de GWCON (Talk 5)(Restablecer interfaz)	467
Uso de IP Versión 6 (IPv6)	469
Visión general de IPv6	469
Comparación de IPv6 con IPv4	469
Direccionamiento de IPv6	470
Formato de dirección de IPv6	470
Representación textual de prefijos de direcciones	471

Formato de cabecera de IPv6	471
MTU mínima de IPv6	471
Path MTU Discovery obligatorio en IPv6	471
Seguridad obligatoria de IPv6	472
IPv6 Neighbor Discovery Protocol (NDP)	472
Router y Prefix Discovery	472
Configuración automática de direcciones	473
Resolución de direcciones	473
Detección de inaccesibilidad de vecinos	473
Redirección	473
Función de túnel de IPv6 sobre IPv4	473
Protocol Independent Multicast (PIM)	474
Configuración y supervisión de IPv6	475
Acceso al entorno de configuración de IPv6	475
Mandatos de configuración de IPv6	475
Add	476
Change	483
Delete	483
Disable	483
Enable	484
List	484
Move	487
Set	487
Update	491
Mandatos de actualización del filtro de paquetes	491
Acceso al entorno de supervisión de IPv6	496
Mandatos de supervisión de IPv6	496
Access-control	497
Cache	497
Counters	498
Vuelco de tablas de direccionamiento	498
Direcciones de interfaz	498
Dirección interna	499
Mcast	499
Mld	499
Reset	500
Route	500
Sizes	500
Sniffer	501
Rutas estáticas	501
Packet-filter	501
Path-mtu	502
Ping6	502
Traceroute6	503
Tunnels	504
Soporte de reconfiguración dinámica de IPv6	504
Delete Interface de CONFIG (Talk 6)(Suprimir interfaz)	504
Activate Interface de GWCON (Talk 5)(Activar interfaz)	504
Reset Interface de GWCON (Talk 5)(Restablecer interfaz)	504
Mandatos Component Reset de GWCON (Talk 5)(Restablecer componente)	504
Mandatos Immediate Change de CONFIG (Talk 6)(Cambio inmediato)	505

Configuración y supervisión de Neighbor Discovery Protocol (NDP) . . .	507
Acceso al entorno de configuración de NDP	507
Mandatos de configuración de NDP	507
Add	508
Change	510
Delete	512
Disable	512
Enable	512
List	512
Set	513
Acceso al entorno de supervisión de NDP	513
Mandatos de supervisión de NDP	514
DHCPv6-Relay	514
Dump	514
List	514
Ping6	515
Soporte de reconfiguración dinámica de NDP6	515
Delete Interface de CONFIG (Talk 6)(Suprimir interfaz)	515
Activate Interface de GWCON (Talk 5)(Activar interfaz)	515
Reset Interface de GWCON (Talk 5)(Restablecer interfaz)	516
Mandatos Component Reset de GWCON (Talk 5)(Restablecer componente)	516
 Configuración y supervisión de Protocol Independent Multicast Routing Protocol (PIM)	 517
Uso de PIM	517
Acceso al entorno de configuración de PIM	518
Mandatos de configuración de PIM	518
Delete	519
Disable	519
Enable	519
List	519
Set	521
Acceso al entorno de supervisión de PIM	523
Mandatos de supervisión de PIM	524
Dump routing tables	524
Clear	525
Interface	525
Join	526
Leave	526
Mcache	526
Mgroups	527
Mstats	527
Neighbor	529
PIM	530
Summary PIM	530
Ping	531
Reset	531
Traceroute	531
Variables	531
Soporte de reconfiguración dinámica de PIM	532
Delete Interface de CONFIG (Talk 6)(Suprimir interfaz)	532
Activate Interface de GWCON (Talk 5)(Activar interfaz)	532
Reset Interface de GWCON (Talk 5)(Restablecer interfaz)	533

Mandatos Component Reset de GWCON (Talk 5)(Restablecer componente)	533
Soporte de reconfiguración dinámica de PIM para IPv6	533
Delete Interface de CONFIG (Talk 6)(Suprimir interfaz)	533
Activate Interface de GWCON (Talk 5)(Activar interfaz)	533
Reset Interface de GWCON (Talk 5)(Restablecer interfaz)	534
Mandatos Component Reset de GWCON (Talk 5)(Restablecer componente)	534
Soporte de reconfiguración dinámica de Multicast Forwarding Cache	534
Delete Interface de CONFIG (Talk 6)(Suprimir interfaz)	534
Activate Interface de GWCON (Talk 5)(Activar interfaz)	535
Reset Interface de GWCON (Talk 5)(Restablecer interfaz)	535
Mandatos no reconfigurables dinámicamente	535
Soporte de reconfiguración dinámica de Multicast Forwarding Cache V6	535
Delete Interface de CONFIG (Talk 6)(Suprimir interfaz)	535
Activate Interface de GWCON (Talk 5)(Activar interfaz)	535
Reset Interface de GWCON (Talk 5)(Restablecer interfaz)	536
Mandatos no reconfigurables dinámicamente	536
Configuración y supervisión de Routing Information Protocol (RIP6)	537
Acceso al entorno de configuración de RIP6	537
Mandatos de configuración de RIP6	537
Add	538
Change	538
Delete	540
Disable	541
Enable	542
List	544
Set	544
Acceso al entorno de supervisión de RIP6	547
Mandatos de supervisión de RIP6	547
Dump	548
List	548
Ping6	548
Reset	548
Traceroute6	548
Soporte de reconfiguración dinámica de RIP6	549
Delete Interface de CONFIG (Talk 6)(Suprimir interfaz)	549
Activate Interface de GWCON (Talk 5)(Activar interfaz)	549
Reset Interface de GWCON (Talk 5)(Restablecer interfaz)	549
Mandatos Component Reset de GWCON (Talk 5)(Restablecer componente)	549
Mandatos Immediate Change de CONFIG (Talk 6)(Cambio inmediato)	550
Mandatos no reconfigurables dinámicamente	550
Configuración y supervisión de BGP6	551
Acceso al entorno de configuración de BGP6	551
Mandatos de configuración de BGP6	551
Add	552
Attach	558
Change	558
Delete	560
Disable	562
Enable	562

List	563
Move	565
Set	566
Update	566
Acceso al entorno de supervisión de BGP6	568
Mandatos de supervisión de BGP6	568
Disable Neighbor	569
Dump Routing Tables	570
Enable Neighbor	570
List	570
Neighbors	573
Parameter	575
Paths	575
Ping6	576
Policy-List	576
Reset Neighbor	577
Sizes	577
Traceroute6	577
Soporte de reconfiguración dinámica de BGP6	577
Delete Interface de CONFIG (Talk 6)(Suprimir interfaz)	578
Activate Interface de GWCON (Talk 5)(Activar interfaz)	578
Reset Interface de GWCON (Talk 5)(Restablecer interfaz)	578
Mandatos Component Reset de GWCON (Talk 5)(Restablecer componente)	578
Mandatos de cambio temporal de GWCON (Talk 5)	578
Mandatos no reconfigurables dinámicamente	579
Apéndice A. Comparación de protocolos	581
Tabla de comparación de los protocolos	581
Clave para los protocolos	581
Apéndice B. Tamaños de los paquetes	583
Cuestiones generales	583
Límites de tamaño específicos de la red	583
Límites de tamaño específicos del protocolo	584
Longitudes de paquete IP	584
Cambio de los tamaños máximos de paquete	585
Apéndice C. Lista de Abreviaturas	587
Glosario	597
Índice	625

Figuras

1.	Conectividad de Extended Border Node	18
2.	Flujo de datos en una configuración de APPN cuando se usa un puerto DLSw	45
3.	Vista lógica con soporte de red de conexiones BAN/Trama puenteadada Frame Relay	46
4.	Trama puenteadada de APPN Frame Relay con la red de conexiones BAN	47
5.	Red de conexiones única que usa BAN con 1 puerto de Frame Relay	48
6.	Red de conexiones única que usa BAN con varios puertos Frame Relay	48
7.	Diversas redes de conexiones que usan BAN	48
8.	Red de conexiones única que usa el puenteo con 1 puerto de Frame Relay	49
9.	Red de conexiones única que usa el puenteo con diversos puertos Frame Relay	49
10.	Diversas redes de conexiones que usan el puenteo	50
11.	Ejemplo de filtro de zonas	290
12.	Ejemplo de filtro de red	292
13.	Tabla de direccionamientos de ejemplo	311
14.	Tabla de vecinos de ejemplo	312
15.	Ejemplo de un control de acceso incluyente	334
16.	Ejemplo de control de acceso excluyente	335
17.	Ejemplo de filtro de direccionamiento de áreas para seguridad	337
18.	Ejemplo de fusión de dominios de DECnet	340
19.	Red OSI	367
20.	Estructura de dirección de NSAP	368
21.	Interpretación de direccionamiento NSAP IS-IS	369
22.	Formato de dirección GOSIP	370
23.	Dominio OSI	373
24.	Áreas sinónimas	374
25.	Métricas de direccionamiento externo e interno	380
26.	Visión general de Next Hop Resolution Protocol (NHRP)	433
27.	NHRP en un entorno Classic IP	436
28.	NHRP en un entorno Classic IP con dispositivos no capacitados para NHRP	437
29.	NHRP en un entorno ELAN	438
30.	NHRP en un entorno ELAN con conmutadores de LAN	439
31.	NHRP en un entorno ELAN o classical IP mixto	439
32.	NHRP a un direccionador de salida	440
33.	Uso de atajos de direccionador a direccionador no permitidos	445

Tablas

1.	Implementación de funciones de nodo de red APPN	4
2.	Tipos de puerto con soporte para direccionamiento de APPN	23
3.	Valores de tipo de dispositivo/modelo	101
4.	Resumen de los mandatos de configuración de APPN	117
5.	Lista de parámetros de configuración - Direccionamiento de APPN	119
6.	Lista de parámetros de configuración - Direccionamiento de alto rendimiento (HPR)	125
7.	Lista de parámetros de configuración - Temporizador de HPR y opciones de reintento	125
8.	Lista de parámetros de configuración - Peticionario de LU dependientes	128
9.	Lista de parámetros de configuración - Ajuste del nodo APPN	131
10.	Lista de parámetros de configuración - Preguntas de configuración de los rastreos	136
11.	Lista de parámetros de configuración - Rastreos de nivel de nodo	137
12.	Lista de parámetros de configuración - Rastreos de señales entre procesos	141
13.	Lista de parámetros de configuración - Rastreos de la entrada y salida en módulos	144
14.	Lista de parámetros de configuración - Rastreos de nivel de componentes generales	146
15.	Lista de parámetros de configuración - Rastreos varios	150
16.	Lista de parámetros de configuración - Gestión de nodos APPN	152
17.	Lista de parámetros de configuración - Soportes de registro de APPN ISR	153
18.	Lista de parámetros de configuración - Configuración de puertos	155
19.	Lista de parámetros de configuración - Configuración de puerto para ATM	158
20.	Lista de parámetros de configuración - Definición de puertos	163
21.	Lista de parámetros de configuración - Características del TG del puerto por omisión	167
22.	Lista de parámetros de configuración - Características LLC del puerto por omisión	172
23.	Lista de parámetros de configuración - Valores por omisión de la alteración temporal de HPR	175
24.	Lista de parámetros de configuración - Estaciones de enlace - Detalle	176
25.	Lista de parámetros de configuración - Configuración de estación para ATM	186
26.	Lista de parámetros de configuración - Modificación de las características de los TG	190
27.	Lista de parámetros de configuración - Modificación del servidor de LU dependientes	192
28.	Lista de parámetros de configuración - Modificación de las características del LLC	193
29.	Lista de parámetros de configuración - Modificación de los valores por omisión de HPR	195
30.	Lista de parámetros de configuración - Nombre de la LU del nodo final LEN	197
31.	Lista de parámetros de configuración - Red de conexiones - Detalle	198
32.	Lista de parámetros de configuración - Configuración de la red de conexiones para ATM	200

33.	Lista de parámetros de configuración - Características de los TG (red de conexiones)	203
34.	Lista de parámetros de configuración - APPN COS - Correlación del nombre de modalidad con el nombre de COS - Detalle	206
35.	Lista de parámetros de configuración - Puerto adicional APPN a red de conexiones	207
36.	Lista de parámetros de configuración - Punto focal implícito de APPN	208
37.	Lista de parámetros de configuración - PU local de APPN	208
38.	Lista de parámetros de configuración - Configuración de la lista de direccionamientos	211
39.	Lista de parámetros de configuración - Configuración de la tabla de correlaciones de COS	215
40.	Resumen de los mandatos de configuración de TN3270E	218
41.	Lista de parámetros de configuración - Establecimiento de TN3270E	218
42.	Lista de parámetros de configuración - Añadir TN3270E implícito	221
43.	Lista de parámetros de configuración - Añadir LU TN3270E	223
44.	Lista de parámetros de configuración - Añadir correlación de TN3270E	226
45.	Lista de parámetros de configuración - Añadir puerto de TN3270E	227
46.	Lista de parámetros de configuración - Suprimir LU de TN3270E	228
47.	Lista de parámetros de configuración - Supresión de TN3270E implícita	228
48.	Lista de parámetros de configuración - Suprimir correlación de TN3270E	229
49.	Lista de parámetros de configuración - Suprimir puerto de TN3270E	230
50.	Resumen de los mandatos de supervisión de APPN	231
51.	Resumen de los mandatos de supervisión del servidor de TN3270E	233
52.	Distintivos	235
53.	Descripción de la salida de APING	236
54.	Descripción de la salida de list appc_sessions	238
55.	Descripción de la salida	239
56.	Descripción de la salida de list dlur-dlus	240
57.	Descripción de la salida de list dlur lu	240
58.	Descripción de la salida	241
59.	Descripción de la salida	243
60.	Descripción de la salida	243
61.	Descripción de la salida	244
62.	Descripción de la salida	245
63.	Descripción de la salida	245
64.	Descripción de la salida	246
65.	Descripción de la salida	247
66.	Descripción de la salida	249
67.	Descripción de la salida	250
68.	Descripción de la salida	251
69.	Descripción de la salida	252
70.	Tabla de asociados	253
71.	Tabla de conexiones	253
72.	Descripción de la salida	255
73.	Descripción de la salida	257
74.	Descripción de la salida	258
75.	Descripción de la salida	259
76.	Descripción de la salida	260
77.	Descripción de la salida	261
78.	Descripción de la salida	261
79.	Descripción de la salida	262
80.	Sintaxis del submenú de Log view	263
81.	Descripción de la salida (Página de resumen, de izquierda a derecha)	264

82.	Descripción de la salida (Detalles del suceso)	265
83.	Descripción de la salida	267
84.	Descripción de la salida	269
85.	Descripción de la salida	270
86.	Resumen de los mandatos de supervisión de TN3270E	271
87.	Descripción de los distintivos	273
88.	Descripción de la salida	273
89.	Descripción de la salida	274
90.	Descripción de la salida	275
91.	Descripción de la salida	276
92.	Descripción de la salida	277
93.	Descripción de la salida	278
94.	Descripción de la salida	279
95.	Descripción de la salida	280
96.	Descripción de la salida	281
97.	Descripción de la salida	281
98.	Resumen de mandatos de configuración de AppleTalk Phase 2	293
99.	Resumen de los mandatos de supervisión de AppleTalk Phase 2	302
100.	Resumen de los campos de la cabecera de Vines IP	309
101.	Estados VINES ARP de los nodos de servicio y cliente	314
102.	Resumen de los mandatos de configuración de VINES	317
103.	Resumen de los mandatos de supervisión de VINES	321
104.	Consideraciones de algoritmo de DNA IV y DNA V	341
105.	Mandatos de configuración y supervisión de NCP	345
106.	Direcciones de difusión múltiple IS-IS	371
107.	Resumen de mandatos de configuración de OSI	387
108.	Resumen de los mandatos de supervisión de OSI/DECnet V	415
109.	Resumen de mandatos de configuración de NHRP	449
110.	Resumen de los mandatos de configuración avanzada de NHRP	451
111.	Resumen de los mandatos de supervisión de NHRP	460
112.	Resumen de los parámetros de configuración de NHRP	464
113.	Resumen de los mandatos de configuración de IPv6	475
114.	Resumen de los mandatos de configuración del filtro de paquetes	491
115.	Resumen de los mandatos de supervisión de IPv6	496
116.	Resumen de mandatos de configuración de NDP	507
117.	Resumen de los mandatos de supervisión de NDP	514
118.	Resumen de los mandatos de configuración de PIM	519
119.	Resumen de mandatos de supervisión de PIM	524
120.	Resumen de los mandatos de configuración de RIP6	537
121.	Resumen de los mandatos de supervisión de RIP6	547
122.	Resumen de los mandatos de configuración de BGP6	551
123.	Resumen de los mandatos de supervisión de BGP6	569
124.	Comparación de protocolos	581
125.	Clave para los protocolos	581
126.	Tamaño máximo por omisión del paquete específico de red	583

Avisos

Puede que IBM no ofrezca en otros países los productos, servicios o características que se mencionan en este documento. Póngase en contacto con el representante local de IBM si desea obtener información de los productos y servicios disponibles actualmente en su país. 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. Se pueden enviar consultas sobre licencias por escrito a:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Para consultas sobre licencias referentes a información de bit doble (DBCS), póngase en contacto con el Departamento de propiedad intelectual de IBM en su país o envíelas por escrito a:

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

El párrafo siguiente no es aplicable al Reino Unido ni a ningún otro país donde su contenido entre en contradicción con la ley local: INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL", SIN GARANTÍAS DE NINGÚN TIPO, NI EXPLÍCITAS NI IMPLÍCITAS, INCLUYENDO PERO NO LIMITÁNDOSE A LAS GARANTÍAS IMPLÍCITAS DE NO INFRACCIÓN, COMERCIALIZACIÓN O IDONEIDAD PARA UN PROPÓSITO DETERMINADO. Algunos estados no autorizan la exclusión de garantías explícitas ni implícitas en determinadas transacciones, por lo que es posible que este aviso no sea aplicable en su caso.

Marcas registradas

Los términos siguientes son marcas registradas de International Business 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 registradas 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 pertenece a la biblioteca de productos descrita en “Publicaciones de IBM 2210 Nways Multiprotocol Router” en la página xxv y describe un grupo de protocolos que tienen soporte de 2210. Puede que un 2210 específico no dé soporte a todas las características y funciones descritas en los presentes manuales. Si una característica o función es específica de un dispositivo, esta restricción se indicará en el manual pertinente.

Este manual hace referencia al 2210 como “direccionador” o “dispositivo.” Los ejemplos de la biblioteca representan la configuración de un 2210, pero la salida real que se verá puede variar. Use los ejemplos como directriz de lo que puede ver mientras configura el dispositivo.

Quién debe leer este manual

Este manual está destinado a aquellas personas que instalan y operan redes de sistemas. Aunque la experiencia con hardware y software de red de sistemas es útil, no es necesario tener experiencia en programación para usar el software de protocolo.

Obtención de información adicional

Pueden efectuarse cambios en la documentación después de que se impriman los manuales. Si hay información adicional disponible o si es necesario realizar cambios después de la impresión de los libros, dichos cambios se encontrarán en un archivo (denominado README) del CD-ROM. Podrá visualizar el archivo con un editor de texto de código ASCII.

Acerca del software

IBM Nways Multiprotocol Routing Services es el software que da soporte al IBM 2210 (número de programa bajo licencia 5801-ARR). 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 Routing 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 2210.

- El programa de configuración Programa de configuración para IBM Nways Multiprotocol Routing 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 Routing Services a partir de la página de presentación del soporte técnico de la red de IBM. Consulte el manual *Configuration Program User's Guide for Nways Multiprotocol and Access Services*, GC10-3430, si desea obtener los directorios y la dirección de servidor.

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 pulsán se indican así: **Intro**

7. Las variables (es decir, nombres utilizados para representar datos que define el usuario) aparecen en letra cursiva. Por ejemplo:

```
Nombre de archivo: nombarchivo.ext
```

Publicaciones de IBM 2210 Nways Multiprotocol Router

Reorganización de la biblioteca: A partir de la versión 3.2, han tenido lugar los siguientes cambios en la organización de la biblioteca:

- La información del manual *Guía del usuario de software* con el título de **Understanding, Using and Configuring Features** ha pasado a un nuevo manual, *Using and Configuring Features*.
- Los capítulos sobre la utilización, configuración y supervisión de la función DIAL han pasado al manual *Using and Configuring Features*.

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 la página de presentación sobre redes de IBM en:

<http://www.networking.ibm.com>

La lista siguiente muestra los manuales que dan soporte al IBM 2210.

Gestión de red y operaciones

SC10-3427 *Guía del usuario de software*

En este manual se explica cómo:

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

SC10-3429 *Using and Configuring Features*

SC10-3426 *Consulta de configuración y supervisión de protocolos Volumen 1*

SC10-3428 *Consulta de configuración y supervisión de protocolos Volumen 2*

Estos manuales describen cómo acceder a la interfaz de usuario de direccionador de línea de mandatos de Multiprotocol Routing Services y cómo utilizarla para configurar y supervisar el software de protocolo de direccionamiento y las funciones que se han suministrado con el direccionador.

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 descripciones y acciones recomendadas para corregir los errores.

Configuración

Resumen de los cambios

Ayuda en línea

Los paneles de ayuda del Configuration Program ayudan al usuario a comprender las funciones del programa y sus paneles, parámetros de configuración y teclas de navegación.

GC10-3430 *Configuration Program User's Guide for Nways Multiprotocol and Access Services*

Este manual describe cómo utilizar el Programa de configuración.

GG24-4446 *IBM 2210 Nways Multiprotocol Router Description and Configuration Scenarios*

Este manual contiene ejemplos de cómo configurar protocolos utilizando IBM Nways Multiprotocol Routing Services.

Seguridad

SD21-0030 *Caution: Safety Information - Read This First*

Este manual proporciona traducciones de avisos de precaución y peligro aplicables a la instalación y al mantenimiento de un IBM 2210.

La lista siguiente muestra los manuales de la biblioteca de IBM 2210 Nways Multiprotocol Router agrupados según las tareas.

Planificación e instalación

GA27-4068 *IBM 2210 Introduction and Planning Guide*

GC30-3867 *IBM 2210 Nways Multiprotocol Router Installation and Initial Configuration Guide*

Estos manuales se suministran con el 2210. En ellos se ofrece una explicación de cómo efectuar los preparativos para la instalación, instalar el 2210, realizar una configuración inicial y verificar si la instalación es satisfactoria.

Estos manuales proporcionan traducciones de avisos de peligro y otra información de seguridad.

Diagnósticos y mantenimiento

SY27-0345 *IBM 2210 Nways Multiprotocol Router Service and Maintenance Manual*

Este manual se suministra con el 2210. Proporciona instrucciones para diagnosticar problemas del 2210 y repararlo.

Resumen de los cambios para la biblioteca de software de IBM 2210

La lista siguiente es aplicable a los cambios que se han efectuado en la Versión 3 Release 4 con respecto al software:

- Mejoras en Frame Relay:
 - Nuevo soporte de Frame Handler (FH)
 - Regulador de PU para manejar las ráfagas de tráfico como soporte de los controladores 3745
 - Nuevo tipo de interfaz (subinterfaz de Frame Relay) para permitir las interfaces virtuales en la misma interfaz física

- Soporte de IP sin numerar
- Mejoras en VPN:
 - Mejoras en CPE:
 - La información de política de los servidores LDAP se almacena localmente.
 - Configuración rápida de política.
 - Comprobación de coherencia de política.
 - La información de política ahora se puede recuperar de los servidores LDAP de dentro de un dominio administrativo.
 - Ping de túnel IPSec.
 - Mejoras en IP:
 - Mejoras en el direccionamiento de voz:
 - Compresión de encabezamientos IP en PPP (RFC 2507, 2508, 2509)
 - Tráfico de voz de interposición entre paquetes de datos fragmentados en PPP de varios enlaces
 - Tráfico de voz de interposición entre paquetes de datos fragmentados en Frame Relay
 - Ignorar PPP o la compresión de paquetes de Frame Relay y cifrado para el tráfico de voz
 - Dirección IP de bucle de retorno

Este soporte permite a los usuarios definir direcciones IP de una interfaz especial para soportar los requisitos de IPSec, TN3270 Gateway y Network Dispatcher.
 - IPv6
 - Se proporciona una función de direccionamiento entre dominios (BGP4+) para IPv6 que da soporte al direccionamiento IPv6 y a la información de direccionamiento y que utiliza TCP6 para el transporte.
 - Se da soporte al tráfico IPv6 a través de una emulación de LAN en ethernet ATM sin encapsulación ni función de túnel.
 - Múltiples vías de reenvío

El direccionamiento IP puede utilizar hasta cuatro rutas estáticas de idéntico coste para dar soporte a varios enlaces paralelos con una dirección y máscara determinadas.
 - Adición de rutas IP
 - Mejoras en difusión múltiple:
 - Protocol Independent Multicast-Modalidad densa (PIM-DM) para IPv4.
 - Ahora los administradores de red pueden controlar el flujo de los datos de difusión múltiple IP que entran y salen de las redes, utilizando los filtros de tráfico de entrada y de salida.
 - Not-so-stubby area (NSSA)

OSPF da soporte a not-so-stubby area (NSSA) tal como se define en la RFC 1587 y el borrador más reciente de Internet ahora está soportado.

Resumen de los cambios

- Detección anticipada aleatoria (RED)
- Mejoras de vigilancia de los servicios diferenciales
- Mejoras en VRRP:
 - La dirección MAC de hardware puede utilizarse en lugar de una dirección MAC virtual para identificar una pasarela redundante; esto puede mejorar el rendimiento.
 - Cuando hay más de un candidato de seguridad disponible, pueden configurarse las opciones prioritarias.
 - Para seleccionar el direccionador de IP original, pueden utilizarse criterios adicionales como por ejemplo interfaz de red o ruta disponible.
- Interfaz alternativa de marcado a solicitud para el redireccionamiento de WAN
- Mejoras en TN3270
 - Limitación de LU
 - Equilibrio de carga de la agrupación de LU
 - Desconexión Talk 5 de las sesiones de TN3270
 - Información adicional
 - Soporte de las direcciones 1 y 255
- Mejoras en Network Dispatcher
 - Anuncio de direcciones de grupo de Network Dispatcher por parte de protocolos de direccionamiento
 - Un nuevo consejero SSL
- Soporte DLSw SDLC PU1
- Soporte de encapsulación ethernet tanto para ethernet tipo II (valor por omisión) como 802.3 simultáneamente en la misma interfaz
- Mejoras de DHCP:
 - Copia de seguridad del disco fijo para información de arriendo
 - Soporte de múltiples direcciones IP para interfaces DHCP
 - Soporte de arriendo corto
- Mejoras en RADIUS
 - Escalabilidad de radio
 - Conexión del último punto de reunión
- Escalabilidad de L2TP
- Mejora en Thin Server
 - Conexión con un servidor alternativo u original de seguridad
- Mejoras de recuperación de archivos de servicio

Aclaraciones y correcciones

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

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 2210 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).

Uso de APPN

En este capítulo se describe APPN® y se incluyen las secciones siguientes:

- “¿Qué es APPN?”
- “¿Qué funciones de APPN se implementan en el direccionador?” en la página 4
- “Características opcionales del nodo de red APPN” en la página 7
- “DLC con soporte” en la página 23
- “Proceso de configuración del direccionador” en la página 24
- “Notas sobre la configuración de APPN” en la página 51

¿Qué es APPN?

Advanced Peer-to-Peer Networking® (APPN) amplía la arquitectura SNA habilitando los nodos de tipo 2.1 (T2.1) para que puedan comunicarse directamente sin tener que recurrir a los servicios de un sistema principal SNA.

Comunicaciones de igual a igual

Los nodos T2.1 pueden activar conexiones con otros nodos T2.1 y establecer sesiones de LU-LU con otros nodos. La relación existente entre un par de nodos T2.1 es conocida como *peer relationship* (relación de iguales) ya que ambas partes pueden iniciar la comunicación.

Antes de APPN, un nodo T2.1 podía comunicarse directamente con otro nodo T2.1, pero debía recurrir a los servicios de un sistema principal SNA centralizado para localizar su pareja y cualquier recurso asociado. Todas las rutas entre ambos nodos estaban definidas previamente. APPN ha mejorado la función del nodo T2.1:

- Haciendo que los recursos de la red sólo se definan en el nodo donde están situados
- Distribuyendo información acerca de estos recursos por toda la red siempre que sea necesario
- Generando dinámicamente rutas entre nodos, usando información actual sobre la topología de la red y la clase de servicio deseado

Tipos de nodos APPN

La arquitectura APPN permite cuatro tipos de nodos en la red:

- Nodos de red APPN
- Nodos finales APPN
- Nodos finales de red de entrada limitada (LEN)
- Nodos PU 2.0 con soporte del DLUR

El direccionador puede configurarse como un nodo de red APPN que da soporte a conexiones con los cuatro tipos de nodos. Sin embargo, no puede funcionar como nodo final para APPN.

Nodo de red APPN

Un nodo de red APPN proporciona servicios de directorio y de direccionamiento para todos los recursos (LU) de su dominio. Un dominio de un nodo de red está formado por:

- Recursos locales propiedad del nodo
- Un punto de control (CP), que gestiona los recursos del nodo
- Recursos propiedad de nodos finales APPN y LEN que usan los servicios del nodo de red

Los nodos de red APPN también:

- Intercambian información acerca de la topología de la red. Esta información se intercambia cada vez que nodos de red establecen una conexión o cuando se produce un cambio en la topología de la red (como, por ejemplo, cuando se desactiva o se pone en línea un nodo de red o cuando un enlace está congestionado o falla). Cuando un nodo de red recibe una actualización topológica, difunde esta información a otros nodos de red activos con los que tiene sesiones de CP-CP.
- Actúan como nodos intermedios, ya que reciben datos de sesión de un nodo adyacente y los pasan al siguiente nodo adyacente en la ruta.

En su calidad de nodo de red, el direccionador también puede actuar como servidor de nodos finales APPN y LEN conectados y proporcionar funciones que incluyen:

Servicios de directorio

El nodo de red, que comunica con otros nodos de red, puede localizar un recurso de ésta en nombre de un nodo final APPN. El nodo de red también mantiene un directorio local de recursos de nodos finales APPN y LEN en el que puede efectuar búsquedas en nombre de un nodo final APPN o LEN conectado u otros nodos de red.

Servicios de topología y direccionamiento

A petición de un nodo final APPN, el nodo de red determina dinámicamente la ruta desde una unidad lógica de origen (LU) a otra de destino en la red. El nodo de red también mantiene información sobre otros nodos de red y las rutas a dichos nodos. La ruta está basada en la topología actual de la red.

Servicios de gestión

El nodo de red puede pasar condiciones de *alerta* a un punto focal designado para permitir una gestión centralizada del problema. Este tipo de nodo es responsable de procesar las condiciones de alerta para todos los recursos de su dominio. “Gestión de un nodo de red” en la página 20 describe este proceso.

Nodos finales APPN

Un nodo final APPN proporciona servicios limitados de directorio, direccionamiento y gestión a las unidades lógicas (LU) asociadas a él. Este tipo de nodo selecciona un nodo de red para que sea su servidor de nodos de la red. Si el nodo de red está de acuerdo en actuar como servidor del nodo final APPN, éste podrá registrar sus recursos locales en el nodo de red. Esto permitirá que el servidor de nodos de la red intercepte y pase peticiones de búsqueda para los recursos situados en el nodo final APPN.

El nodo final APPN y el servidor de nodos de la red se comunican estableciendo sesiones de CP-CP. Un nodo final APPN puede estar conectado a varios nodos de red, pero sólo uno de estos nodos actuará de servidor del mencionado nodo final en cualquier momento.

El nodo final APPN reenvía todas las peticiones de recursos desconocidos al servidor de nodos de la red. A su vez, dicho servidor usa recursos de búsqueda propios para localizar el recurso solicitado y establecer una ruta desde el nodo final APPN hasta el recurso.

Nodos LEN

Un nodo LEN es un nodo T2.1 sin extensiones APPN. Este nodo puede establecer conexiones de igual con otros nodos LEN, nodos finales APPN y nodos de red APPN, siempre que todas las LU de destino necesarias estén registradas en él. Un nodo LEN también puede servir de pasarela entre una red APPN y una red de subárea SNA.

Dado que un nodo LEN no puede establecer sesiones de CP-CP con un servidor de nodos de red APPN, no puede registrar los recursos propios en el servidor o solicitar que éste busque un recurso y establezca dinámicamente una ruta a dicho recurso. Un nodo LEN puede usar indirectamente los servicios de directorio y direccionamiento de un nodo de red definiendo previamente LU remotas (propiedad de nodos que no son adyacentes) como si estuvieran situadas en un nodo de red APPN, aunque estén realmente en cualquier punto de la red. Cuando el nodo LEN necesite iniciar una sesión con la LU remota, el nodo enviará una solicitud de activación de sesión (BIND) para la LU al nodo de red. En dicho caso, el nodo de red actuará como el servidor de nodos de la red del nodo LEN, localizando el recurso solicitado, estableciendo una ruta y reenviando el BIND a su destino correcto.

Cuando configure el nodo de red del direccionador, podrá especificar los nombres de LU asociadas a un nodo final LEN conectado. Estos nombres de LU residen en el directorio local del nodo de red del direccionador. Si el nodo de red del direccionador recibe una solicitud de buscar uno de estos recursos de nodo final LEN, podrá encontrar la LU en el directorio local y dar una respuesta positiva al nodo que ha originado la búsqueda. Para reducir el número de nombres de LU que debe especificar para un nodo final LEN conectado, el direccionador da soporte al uso de nombres de LU genéricos, lo que permite usar un carácter comodín para representar una parte de un nombre LU.

Nodos PU 2.0

Un nodo PU 2.0 es un nodo de tipo T2.0 que contiene LU dependientes. Estos nodos tienen soporte de la función de peticionario de LU dependientes (DLUR) implementada por un nodo final APPN o un nodo de la red. Los nodos PU 2.0 necesitan los servicios de un punto de control de los servicios del sistema, el cual está disponible a través del nodo APPN habilitado por la función DLUR. Observe que los nodos APPN pueden contener LU dependientes con soporte de la función DLUR. No obstante, el direccionador no contiene LU dependientes.

¿Qué funciones de APPN se implementan en el direccionador?

El direccionador implementa las funciones de la arquitectura básica APPN Release 2 tal como se definen en la Systems Network Architecture APPN Reference (Guía de APPN de la arquitectura de red de sistemas). Las funciones de nodo de red APPN implementadas por el direccionador están resumidas en la Tabla 1. Después de la tabla, encontrará notas sobre funciones específicas. Para obtener una descripción acerca de los servicios de gestión de APPN que tienen soporte del direccionador, consulte “Gestión de un nodo de red” en la página 20.

APPN usa protocolos LU 6.2 para proporcionar conectividad de iguales entre los miembros de una sesión de CP-CP. El nodo de red del direccionador implementa los protocolos LU 6.2 necesarios para las sesiones de CP-CP y aquellos que se usan en sesiones establecidas entre un CP de nodo de la red y su punto focal de gestión de la red. La implementación efectuada por el direccionador de APPN no proporciona una interfaz de programa de aplicación para dar soporte a programas de LU 6.2 escritos por el usuario.

Tabla 1 (Página 1 de 2). Implementación de funciones de nodo de red APPN

Función APPN	Sí	No	Notas
Funciones de soporte y servicios de sesión			
Varias sesiones de CP-CP	X		
Correlación de nombre de modalidad con clase de servicio (CoS)	X		1
Estaciones de enlace de recursos limitados	X		2
Segmentación y ensamblamiento de BIND	X		3
Seguridad de nivel de sesión	X		4
Direccionamiento de sesiones intermedias			
Direccionamiento de sesiones intermedias	X		
Direccionamiento de sesiones de LU dependientes	X		
Ritmo de nivel de sesión adaptable y fijado	X		
Segmentación y ensamblamiento de RU	X		5
Servicios de directorio			
Difusión de búsquedas	X		
Búsquedas dirigidas	X		
Puesta en antememoria del directorio	X		
Almacenamiento seguro de la antememoria de servicios del directorio		X	6
Servidor de directorio central		X	7
Cliente de directorios central	X		7
Registro de las LU EN APPN en el servidor de nodos de la red	X		
Definición de la LU de nodos LEN en el servidor de nodos de la red	X		
Uso de caracteres comodín para definir recursos de nodos LEN conectados	X		
Aceptación de varias situaciones de “resource found” (recurso encontrado)	X		

Tabla 1 (Página 2 de 2). Implementación de funciones de nodo de red APPN

Función APPN	Sí	No	Notas
Servidor de nodo de red para DLUR EN - Conjunto de opciones 1116	X		
Servicios de topología y direccionamiento			
Intercambio de topología	X		
Difusiones periódicas de la topología	X		8
Mantenimiento de la base de datos de la topología	X		9
Reconocimiento de la topología en las sesiones de CP-CP	X		
Cálculo de rutas aleatorio	X		10
Árboles de direccionamiento en antememoria	X		11
Almacenamiento seguro de la base de datos de topología		X	
Mejoras en la recogida de desechos	X		
Conectividad			
Definición de la red de conexiones	X		12
Varios grupos de transmisión	X		
Grupos de transmisión en paralelo	X		
Servicios de gestión			
Soporte a varios dominios (MDS)	X		
Punto focal explícito	X		
Punto focal implícito	X		
Retención de alertas	X		
Sesiones de SSCP-PU con puntos focales		X	
Datos para el diagnóstico de problemas de SNA/MS en las alertas	X		

Notas:

- Los nombres de modalidades nuevas pueden definirse en el direccionador usando la interfaz de la línea de mandatos (Command Line interface). Estos nombres pueden correlacionarse con nombres de definiciones de clases de servicio (CoS) ya existentes o bien con definiciones CoS nuevas, que pueden definirse utilizando la herramienta de configuración.
- Las estaciones de enlace de recursos limitados tienen soporte para:
 - Enlaces de red de conexiones
 - Enlaces X.25 SVC
 - Enlaces PPP que se ejecutan sobre RDSI, V.25bis o V.34
 - Enlaces de Frame Relay que se ejecutan sobre RDSI
 - SVC de ATM
 - Enlaces de red en anillo
 - Enlaces Ethernet
- Cuando el direccionador activa un TG a un nodo adyacente, negocia con dicho nodo el tamaño máximo del mensaje que puede enviarse a través del TG. Si un mensaje BIND tiene un tamaño superior al del mensaje negociado, el

direccionador segmentará el BIND. Sólo se efectuará la segmentación si el nodo adyacente puede volver a ensamblar el BIND. El direccionador da soporte al ensamblaje de BIND.

4. Se puede habilitar una función de seguridad de nivel de sesión para las conexiones establecidas entre el nodo de red del direccionador y un nodo adyacente. Los dos asociados de la conexión necesitan una clave hexadecimal coincidente que permita a cada nodo verificar el asociado antes de establecer la conexión.
5. Cuando se direccionan datos de sesión a un nodo adyacente, el direccionador segmenta una unidad de solicitud/respuesta (RU) si la unidad de mensaje supera el tamaño máximo de mensaje que puede enviarse mediante el grupo de transmisión. Si el direccionador recibe una RU segmentada, el nodo la volverá a ensamblar.
6. Después de localizar satisfactoriamente un recurso en la red APPN, el direccionador almacenará o *pondrá en antememoria* esta información en la base de datos de directorio local para futuros usos. No obstante, el direccionador no guardará estas entradas de directorio puestas en antememoria en un soporte de almacenamiento permanente como, por ejemplo, un disco, para proporcionar una posibilidad de recuperación si falla el nodo.
7. El direccionador no puede utilizarse como servidor de directorio central de una red APPN. No obstante, el direccionador puede usar un servidor de directorio central para obtener información del directorio acerca de la situación de un recurso en la red.
8. A fin de evitar que otros nodos de la red descarten información acerca del direccionador en sus bases de datos de topología, el direccionador crea, cada 5 días, una actualización de base de datos de topología (TDU) sobre sí mismo y los grupos de transmisión de propiedad local y la difunde a los nodos de la red.
9. En la base de datos de topología de la red del direccionador, se asocia un temporizador de intervalos a cada entrada de recurso. Si, en el plazo de 15 días, el direccionador no recibe información acerca de un recurso, descartará de la base de datos la entrada de dicho recurso.
10. Si, desde una LU de origen a otra de destino, hay más de una ruta de menos peso para una determinada clase de servicio, el direccionador seleccionará aleatoriamente una de las rutas para la sesión. Esta práctica ayuda a distribuir el flujo de tráfico de la red.
11. El direccionador mantiene una copia de la base de datos de topología de la red. La base de datos identifica las rutas disponibles hacia otros nodos de la red para una clase determinada de servicio. Cuando el direccionador necesite calcular una ruta a un nodo de la red o a un nodo final adyacente a dicho nodo de la red, usará la información de la base de datos de topología para generar un árbol de direccionamiento al mencionado nodo. El árbol de direccionamiento identificará las rutas óptimas al nodo de red para la clase de servicio requerida.

Cuando el direccionador genera un árbol de direccionamiento nuevo, lo almacena en una antememoria. Al recibir una solicitud de servicio, primero comprobará la antememoria para ver si ya ha calculado una ruta. El uso de la antememoria reduce el número necesario de cálculos de rutas. Cuando el direccionador reciba información de topología que invalide un árbol de

direccionamiento, descartará dicho árbol. Luego volverá a calcularlo cuando lo necesite y pondrá en antememoria el árbol nuevo.

12. El direccionador puede definirse como miembro de una red de conexiones en los puertos de Ethernet, de red en anillo, Frame Relay BAN, Soporte de Enterprise Extender para HPR sobre IP y ATM.

Características opcionales del nodo de red APPN

El direccionador, además de implementar las funciones de arquitectura de APPN básicas, también implementa las torres de conjuntos de opciones y las funciones nuevas siguientes:

- 087** Mejoras de Garbage Collection
- 1002** Nombre de la estación de enlace adyacente
- 1007** TG paralelos*
- 1012** Nombre LU = Nombre CP
- 1016** Extended Border Node
- 1061** Requisitos previos de las Extensiones SS para soporte NNS
- 1063** Soporte NNS de las extensiones SS
- 1067** Peticionario de LU dependientes
- 1071** Uso generalizado de ODAI
- 1101** Antememoria de directorios cargada previamente
- 1107** Registro central de recursos (de LU)
- 1116** Soporte del servidor de nodos de la red al registro de LU servido por el DLUS
- 1119** Informe de la topología de ramas a un gestor
- 1120** Branch Awareness
- 1121** Branch Extender
- 1124** Copia de seguridad de Branch Extender con autoconfiguración
- 1200** Puesta en antememoria de árboles y de TG
- 1400** Direccionamiento de alto rendimiento (HPR)
- 1401** Rapid Transport Protocol (RTP)
- 1402** Flujos de control sobre RTP
- 1405** HPR Border Node
 - Ajuste del rendimiento del nodo
 - Rastreo de servicios del nodo
 - Captación de estadísticas de nodo y de contabilidad

***Nota:** Al definir TG paralelos si se utiliza la asignación de números de TG dinámica, deben definirse TODOS o NINGUNO de los enlaces entre los dos nodos.

Direccionamiento de alto rendimiento

HPR es una mejora efectuada en la arquitectura de APPN que proporciona un mejor rendimiento en los enlaces con un índice bajo de errores y alta velocidad, usando el hardware existente. El HPR sustituye al direccionamiento de sesiones intermedias (ISR) de APPN normal por una capa de control de la red (Network Control Layer) (NCL) que contiene un tipo nuevo de función de direccionamiento de origen llamado direccionamiento de red automático (automatic network routing) (ANR). La ruta HPR completa está contenida en el paquete de ANR, lo que permite a los nodos de direccionamiento intermedios direccionar los paquetes con menos sobrecarga de proceso y almacenamiento.

HPR también elimina los procedimientos de control de flujo (ritmo de nivel de sesión)/congestión y recuperación de errores de cada enlace entre nodos y los desplaza a los puntos finales de una conexión HPR. Los puntos finales de dicha conexión usan una capa de transporte la cual, a su vez, usa un procedimiento de recuperación de errores nuevo llamado Rapid Transport Protocol (RTP). Los nodos intermedios de HPR no detectan si están en una conexión RTP o no están en ninguna sesión. Esta capa de transporte nueva tiene las funciones siguientes:

- Un procedimiento de recuperación de errores de transmisión selectivo
- Segmentación y ensamblaje
- Un mecanismo de control de la congestión y del flujo Adaptive Rate-Based (Basado en el ritmo de adaptación - ARB) que mide los datos de una ruta y permite usar eficazmente los recursos de red, además de minimizar la congestión. ARB usa un enfoque preventivo en vez de reactivo para el control de la congestión y el flujo.
- Una función de conmutación de vías de acceso sin interrupciones (NDPS) que vuelve a direccionar automáticamente el tráfico tras el fallo de un nodo o un enlace sin interrumpir las sesiones del usuario final.
- Detección del bit de notificación de congestión explícita hacia delante (FECN) que permite que el algoritmo de control de la congestión y el flujo basado en el ritmo de adaptación de RTP, ajuste el ritmo de envío de datos. Este algoritmo evita las ráfagas y la congestión de tráfico y mantiene un alto nivel de rendimiento.

El direccionador implementa el ANR y el protocolo de transporte rápido. Por consiguiente, puede funcionar como nodo HPR de direccionamiento intermedio y como nodo de punto final de conexión HPR.

Interoperabilidad

HPR utiliza funciones de control de red APPN, incluyendo el cálculo de rutas de menos peso basado en la clase de servicio (CoS) y en la prioridad de transmisión. HPR interactúa sin problemas con APPN ISR:

- La red se adapta automáticamente a la presencia de nodos de HPR y enlaces habilitados para HPR.
- Una red APPN puede contener cualquier mezcla de enlaces ISR y HPR, aunque los mayores beneficios de HPR se consiguen cuando la red tiene tres o más nodos habilitados para HPR con dos o más enlaces de HPR de fondo a fondo. Esto permite que el nodo HPR medio sea un nodo intermedio HPR y use únicamente direccionamiento ANR, lo que hace que los datos de la sesión se direccionen a través del nodo medio usando únicamente NCL.

- Una ruta de sesión puede estar formada por una combinación de enlaces ISR y HPR.
- HPR usa las mismas características de nodo y de TG para el cálculo de rutas de menos peso que APPN ISR. No se da ninguna importancia especial a los nodos o enlaces de HPR salvo a sus características potencialmente mejoradas (como, por ejemplo, una mayor capacidad si se trata de un enlace de mayor velocidad).

Tipos de tráfico

APPN ISR usa el protocolo QLLC para el control de enlaces de datos directos X.25, el protocolo IEEE 802.2 LLC Type 2 para red en anillo, Ethernet, PPP y Frame Relay y el protocolo SDLC para el control de enlaces de datos SDLC. APPN HPR, que tiene soporte en las redes en anillo, Ethernet, PPP, y Frame Relay, no usa el protocolo LLC Type 2, aunque sí utiliza algunas funciones de una estación de enlace de APPN para la espera de inactividad agotada y el XID. Por consiguiente, se usa una única estación de enlace de APPN para ISR o HPR. Esto hace que, para distinguir entre tráfico ISR y tráfico HPR, se utilicen diferentes mecanismos, según el tipo de DLC:

- Para puertos de red en anillo y Ethernet de LAN:

Cada protocolo que utilice un puerto deberá tener una dirección de SAP única, salvo DLSw (que puede utilizar la misma dirección de SAP que otros protocolos ya que las tramas de DLSw no se destinan a la dirección del MAC local, sino a una dirección DLSw MAC). La estación de enlace de APPN para el tráfico HPR se identifica con una dirección de SAP única (parámetro de la dirección de SAP HPR local). Si se destina tráfico ISR a una estación de enlace, deberá usarse una dirección de SAP diferente (parámetro de dirección de SAP APPN local). El tráfico ISR utiliza tramas LLC Type 2 LAN. El tráfico HPR se maneja igual que las tramas LLC Type 1 LAN y debe tener una dirección de SAP diferente.

La dirección de SAP por omisión del tráfico HPR es X'C8'. Si otro protocolo de un puerto ya ha utilizado X'C8', deberá alterarse temporalmente el valor por omisión.

Nota: Sólo hay una estación de enlace de APPN incluso aunque el tráfico APPN HPR y APPN ISR utilicen diferentes direcciones de SAP.

- Para los puertos de Frame Relay:

El tráfico APPN ISR y el APPN HPR transferido en una conexión de enlace de datos Frame Relay dan soporte al formato de trama puenteadada RFC 1490/2427 y al formato de trama direccionado RFC 1490/2427.

- Formato de trama direccionado RFC 1490/2427

El tráfico APPN ISR se transferirá sobre una conexión de enlace de datos Frame Relay usando el método de encapsulación multiprotocolo orientado a la conexión definido en RFC 1490/2427 usando:

- NLPID = X'08' (Codificación Q.933)
- L2PID = X'4C80' (El identificador de protocolo de capa 2 indica 802.2 LLC)
- L3PID = X'7083' (El identificador de protocolo de capa 3 indica SNA-APPN/FID2)

El tráfico APPN HPR transferido sobre una conexión de enlace de datos de frame relay no usa IEEE 802.2 LLC. Utiliza una encapsulación multiprotocolo diferente, tal como se define en RFC 1490/2427, usando:

- NLPID = X'08' (Codificación Q.933)
- L2PID = X'5081' (Identificador de protocolo de capa 2 para ningún protocolo de dicha capa)
- L3PID = X'7085' (El identificador de protocolo de capa 3 indica SNA-APPN/HPR)

APPN HPR no usa el SAP para tráfico transferido usando el formato de trama direccionado RFC 1490/2427, ya que no hay protocolo de capa 2.

- Formato puenteado RFC 1490/2427

APPN HPR usa el SAP para el tráfico transferido usando el formato de trama puenteado RFC 1490/2427.

- Para puertos PPP:
 - El tráfico APPN ISR usa 802.2 LLC sobre la conexión PPP.
 - Dado que en la encapsulación RFC 1490/2427 de HPR no se utiliza ningún protocolo de capa 2, tampoco se usará el SAP para el tráfico HPR.
- Para puertos ATM:
 - El tráfico APPN ISR no tiene soporte en los puertos ATM nativos. No obstante, dos tipos de tráfico APPN tienen soporte, tal como los define RFC 1483:
 - Durante la conexión de la estación de enlace, los XID se transportan usando el formato de trama siguiente:
 - NLPID = X'09'
 - ID del protocolo de capa 2 = X'4C80' (presencia de la cabecera 802.2 LLC)
 - ID del protocolo de capa 3 = X'7083' SNA APPN (FID2) incluyendo XID3
 - El tráfico HPR se transporta usando el formato de trama siguiente:
 - NLPID = X'09'
 - ID del protocolo de capa 2 = X'4C80' (presencia de la cabecera 802.2 LLC)
 - ID del protocolo de capa 3 = X'7085' SNA APPN/HPR (NLP)
- Soporte de Enterprise Extender para HPR sobre IP

Consulte la Tabla 2 en la página 23 para obtener una lista de los DLC que dan soporte a HPR.

Nota: HPR no tiene soporte sobre puertos SDLC, X.25 o DLSw.

Peticionario de LU dependientes (DLUR)

La opción DLUR amplía el soporte de los dispositivos T2.0 ó T2.1 que contienen LU dependientes de nodos APPN. La función DLUR de un nodo de red APPN o un nodo final APPN funciona junto con un servidor de LU dependientes (DLUS) en una red mixta de subárea/APPN. La función DLUS debe residir en alguna otra parte de la red mixta del DLUR.

Los flujos de LU dependientes (SSCP-PU y SSCP-LU) se encapsulan sobre un conducto de LU 6.2 (CP-SVR) establecido entre el nodo DLUR APPN y el DLUS SSCP. El conducto CP-SVR está formado por un par de sesiones de LU 6.2 que usan una modalidad CPSVRMGR nueva entre el DLUR y el DLUS. El conducto lleva la función SSCP (del DLUS) al nodo DLUR APPN donde está a disposición de los nodos T2.0/T2.1 que contienen LU dependientes.

Parecerá que la LU dependiente está situada dentro del dominio del SSCP de servicio. Los flujos de inicio de sesión se emularán desde el DLUS, pero el enlace y las vías de acceso a los datos de la sesión se calcularán directamente entre la LU dependiente y su asociado de sesión. Este recorrido puede o no atravesar el nodo DLUS de servicio.

Establezca el parámetro del tipo de nodo adyacente en PU 2.0 Node (Nodo PU 2.0) cuando defina una estación de enlace a un nodo adyacente T2.0 que contenga LU dependientes. Establezca el parámetro del tipo de nodo adyacente en APPN end node (nodo final APPN) o LEN end node (nodo final LEN) cuando defina una estación de enlace a un nodo adyacente T2.1 que contenga LU dependientes.

Consulte la Tabla 2 en la página 23 para saber cuáles son los tipos de puertos que dan conexión a la PU en sentido directo (DSPU) que tienen soporte.

Funciones con soporte

La opción APPN DLUR incluye las funciones siguientes:

- Soporte a nodos T2.0 en sentido directo conectados a SDLC y que contienen LU dependientes que no dan soporte al intercambio de XID.
- Soporte para nodos T2.0 en sentido directo que contienen LU dependientes que responden con un XID de tipo 0 y un XID de tipo 1.
- Soporte para nodos T2.1 en sentido directo que contienen LU dependientes que responden con un XID de tipo 3.
- Soporte para LU dependientes que equivale al soporte proporcionado por el entorno de subárea para:
 - Activar PU y las LU respectivas
 - Localizar y ser localizado por otras LU en una red de subárea o APPN
 - Determinar las características de las LU
 - Permitir que los operadores de los terminales inicien sesión con aplicaciones en redes APPN y de subárea
 - La entrada en función de SSCP
 - Sesiones ininterrumpidas de LU-LU, si el DLUS de soporte (SSCP) falla
 - Inicializar SLU, inicializar PLU e inicializar terceros

Restricciones

La opción DLUR, tal como se implementa en el nodo de red del direccionador, tiene las siguientes restricciones funcionales:

- Sólo las LU secundarias (SLUs) pueden tener soporte de la función DLUR. Una LU con soporte del DLUR no puede funcionar como LU primaria (PLU). Por consiguiente, la unidad física directa (DSPU) debe configurarse como secundaria.
- Dado que sólo las SLU tienen soporte, no se da soporte a Network Routing Facility (NRF) ni a Network Terminal Option (NTO).

- El recurso de recuperación ampliada (XRF) y XRF/CRYPTO no tienen soporte.
- Debe ser posible establecer una sesión sólo de APPN/HPR o sólo de APPN entre DLUS y DLUR. La sesión CPSVRMGR no puede pasar por una red de subárea.

Consideraciones de VTAM para DLUR

A continuación se encuentra un ejemplo de definiciones de VTAM® Switched Major Node (Nodo principal conmutado de VTAM) para DLUR. Observe que las sentencias PATH sólo son necesarias si VTAM está iniciando la conexión con la DSPU.

Debe consultar el manual *IBM VTAM Resource Definition Reference* (Consulta de definiciones de recursos de VTAM) si desea obtener información sobre las sentencias del parámetro DLC de las definiciones Switched Major Node.

```

DABDLURX VBUILD TYPE=SWNET,MAXGRP=400,MAXNO=400,MAXDLUR=20
*****
*IN THE DLCADDR, THE 'SUBFIELD_ID' = CV SUBFIELD OF THE CV91          *
* MINUS 0X90.                                                         *
*FOR EXAMPLE, THE CV94 SUBFIELD IS CODED ON DLCADDR=(4,X,...         *
*****
* Following are PU Statements for 2.0 and for 2.1
*****
* 2.0 PU STATEMENT
*****
*PU20RT  PU  ADDR=05,PUTYPE=2,MAXPATH=8,ANS=CONT,USSTAB=AUSSTAB,
*           ISTATUS=ACTIVE,MAXDATA=521,IRETRY=YES,MAXOUT=7,
*           PASSLIM=5,IDBLK=017,IDNUM=00035,MODETAB=AMODETAB
*           LOGAPPL=ECH071,DLOGMOD=M23278I  1
*****
* Path statements are not required if the DSPU is initiating the
* connection to VTAM
*****
*PU20LU1  LU  LOCADDR=2  11
*PU20LU2  LU  LOCADDR=3
*PU20LU3  LU  LOCADDR=4
*****
* 2.1 PU STATEMENT
*****
*PU21RT  PU  ADDR=06,PUTYPE=2,CPNAME=PU21RT,ANS=CONT,MAXPATH=8,
*           ISTATUS=ACTIVE,USSTAB=AUSSTAB,MODETAB=AMODETAB
*           LOGAPPL=ECH071,DLOGMOD=M23278I  1
*****
*
* Following are examples of path statement coding for various
* DLC types.
*
* There is no difference in the path statement definitions
* between a PU 2.0 and a PU 2.1
*
* Path statements are required if VTAM is initiating the connection
* to the DSPU.
*
*****
* Below is SDLC
*****
*A20RT  PATH  PID=1,
*           DLURNAME=GREEN,
*           DLCADDR=(1,C,SDLCNS),
*           DLCADDR=(2,X,5353),  2  **nombre puerto
*           DLCADDR=(3,X,C1)    3a  **dirección estación

```

```

*****
* Below is Frame Relay
*****
*A20RT  PATH  PID=2,
*          DLURNAME=GREEN,
*          DLCADDR=(1,C,FRPVC),
*          DLCADDR=(2,X,4652303033),      2 **nombre puerto
*          DLCADDR=(3,X,04),             3 **dirección SAP
*          DLCADDR=(4,X,0024)           4 **DLCI
*****
* Below is Frame Relay BAN
*****
*A20RT  PATH  PID=3,
*          DLURNAME=GREEN,
*          DLCADDR=(1,C,FRPVC),
*          DLCADDR=(2,X,4652303033),      2 **nombre puerto
*          DLCADDR=(3,X,04),             3 **dirección SAP
*          DLCADDR=(4,X,0024),           4 **DLCI
*          DLCADDR=(6,X,40000000001)     5 **dirección MAC
*****
* Below is DLSw
*****
*A20RT  PATH  PID=3,
*          DLURNAME=GOLD,
*          DLCADDR=(1,C,TR), 7
*          DLCADDR=(2,X,444C53323534), 2 **nombre puerto
*          DLCADDR=(3,X,04),             3 **dirección SAP
*          DLCADDR=(4,X,40000000001)     6 **dirección MAC
*
*****
** Below is Token Ring
*****
*PATH20  PATH  PID=1,
*          DLURNAME=RED,
*          DLCADDR=(1,C,TR),
*          DLCADDR=(2,X,5452303030),     2 **nombre puerto
*          DLCADDR=(3,X,04),             3 **dirección SAP
*          DLCADDR=(4,X,400000011088)    6 **dirección MAC
*****
** Below is Ethernet
*****
*PATHE20  PATH  PID=1,
*          DLURNAME=PURPLE,
*          DLCADDR=(1,C,ETHERNET),
*          DLCADDR=(2,X,454E303030),     2 **nombre puerto
*          DLCADDR=(3,X,20),             3 **dirección SAP
*          DLCADDR=(4,X,400000011063)    6 **dirección MAC
*****
* Below is X25 SVC
*****
*A20RT  PATH  PID=3,
*          DLURNAME=GREEN,
*          DLCADDR=(1,C,X25SVC),
*          DLCADDR=(2,X,583235303033),   2 **nombre puerto
*          DLCADDR=(4,X,C3),             3 **Identificador protocolo
*          DLCADDR=(21,X,000566666),    9 **dirección DTE destino
*****
* Below is X25 PVC
*****
*A20RT  PATH  PID=3,
*          DLURNAME=GREEN,
*          DLCADDR=(1,C,X25PVC),
*          DLCADDR=(2,X,583235303033),   2 **nombre puerto
*          DLCADDR=(3,X,0001)           10 **Número canal lógico
*****

```

```
*****  
*****  
* Sentencias de LU  
*****  
*****  
*PU21LU1 LU LOCADDR=2 11  
*PU21LU2 LU LOCADDR=3  
*PU21LU3 LU LOCADDR=4  
*****  
*****
```

Notas:

- 1** La diferencia entre el codificado de sentencias PU es:
 - Para las definiciones de 2.0, la sentencia PU tiene IDBLK=...,IDNUM=....
 - Para las definiciones de 2.1, la sentencia PU tiene CPNAME=....
- 2** Nombre del puerto en ASCII definido en el direccionador y usado por la DSPU
- 3** SAP de la DSPU (no canónica, salvo para Ethernet)
- 3a** Dirección de la estación para SDLC
- 4** DLCI debe tener 4 dígitos ya que es media palabra
- 5** Dirección del MAC de la DSPU (no canónica) para Frame Relay BAN
- 6** Dirección del MAC de la DSPU (no canónica, salvo para la dirección MAC de Ethernet, que es canónica)
- 7** DLSw aparece a VTAM como un DLC de red en anillo
- 8** Identificador de protocolo
- 9** Dirección del DTE de destino (000566666, donde:
00 es fijo
05 es la longitud de la dirección del DTE
66666 es la dirección del DTE)
- 10** Número de canal lógico. Debe tener 4 dígitos ya que es media palabra.
- 11** Codificado de la LU

Consulte “Uso de TN3270” en la página 89 para ver un ejemplo de una sentencia de vía de acceso de PU interna.

Redes de conexiones APPN

Cuando los nodos están conectados a un recurso de transporte de acceso compartido (shared-access transport facility - SATF), se pueden establecer conexiones desde cualquier punto a cualquier punto. Esta conectividad de cualquiera con cualquiera permite establecer conexiones directas entre cualquier par de nodos, con lo que se elimina el direccionamiento a través de nodos de red y que los datos correspondientes atraviesen varias veces el SATF. No obstante, a fin de conseguir esta capacidad de conexión directa, los TG deben estar definidos en cada nodo para el resto de los posibles asociados.

La definición de conexiones entre todos los pares de nodos posibles conectados al SAFT da como resultado un gran número de definiciones (el número de nodos participantes al cuadrado) así como un gran número de actualizaciones de la base de datos de topología (TDU) circulando por la red APPN. A fin de aligerar este problema, APPN permite que los nodos se conviertan en miembros de una red de conexiones para representar su conexión con un SATF. El tráfico de sesión entre dos nodos definidos como miembros de una red de conexiones puede direccionarse directamente, sin pasar a través de un nodo de red (consigue una conectividad directa). Para convertirse en miembro de una red de conexiones, el

puerto de un nodo APPN debe "conectarse" a dicha red definiendo una interfaz de red de conexiones. Una vez definido el puerto, el componente APPN crea un TG de red de conexiones para identificar la conexión directa del puerto al SAFT (por ejemplo, la red de conexiones). Este TG no es un TG convencional en el caso de las estaciones de enlace definidas, sino que representa la conexión a la red de conexiones en la base de datos de topología.

Nota: Los TG para los nodos finales no están contenidos en la base de datos de topología de la red, sino que están en la base de datos de topología local del nodo. Las TDU no circulan por la red cuando se establece una conexión a través de la red de conexiones o cuando un nodo final se convierte en miembro de dicha red.

Dado que la conectividad está representada por un TG de un nodo determinado con una red de conexiones, el servidor de nodos de red puede usar los servicios de direccionamiento y topología normales (TRS) para establecer la vía de acceso directa entre cualquier par de nodos conectados al SAFT (con los TG con la misma red de conexiones). La información de señalización DLC se devuelve desde el nodo de destino durante el proceso de localización normal para habilitar al nodo de origen para que establezca directamente una conexión con el nodo de destino.

Por consiguiente, para conseguir una conectividad directa en un SAFT, en vez de que cada nodo del SAFT se defina (o conecte) con todos los demás, cada nodo se conecta a una red de conexiones. A menudo, se visualiza la red de conexiones como un nodo virtual del SAFT al que están conectados el resto de los nodos. Este modelo se usa con frecuencia y, de hecho, el término Virtual Routing Node (Nodo de direccionamiento virtual - VRN) se utiliza a menudo en lugar del término red de conexiones.

Cuando se define una red de conexiones, se le da un nombre. Este nombre se convierte en el nombre del CP del VRN y debe cumplir todos los requisitos de cualquier nombre de CP. Consulte la Tabla 24 en la página 176 para obtener una lista de los mencionados requisitos.

Restricciones

- La misma red de conexiones (VRN) puede definirse en una única LAN. No obstante, esta red puede definirse en varios puertos que tengan las mismas características con la misma LAN.
- Sólo hay un TG de red de conexiones desde un puerto determinado a un VRN de red de conexiones determinada.
- Dado que un VRN no es un nodo real, no pueden establecerse sesiones de CP-CP con el VRN o a través de éste.
- Cuando se define una red de conexiones en el nodo de red del direccionador, se especifica un nombre plenamente calificado para el parámetro *connection network name* (nombre de la red de conexiones). Sólo pueden definirse las redes de conexiones con el mismo ID de red que el nodo de red del direccionador. El ID de red de VRN será, entonces, el mismo que el ID de red del nodo de red del direccionador.

Branch Extender

La función Branch Extender (BrNN) ha sido diseñada para optimizar la conexión de una filial con la red troncal APPN WAN. Esta función aísla a todos los nodos finales de una o varias LAN de filiales, de la WAN troncal. El dominio de una BrNN puede contener únicamente nodos finales y BrNN en cascada. El dominio de una BrNN no contiene nodos de red o nodos con DLUR.

Cuando configure una BrNN, configure las estaciones de enlace con la red troncal para que sean enlaces de hacia arriba. Esto hará que la función BrNN aparezca como un nodo final convencional de la red troncal. Desde la perspectiva de dicha red, todos los recursos de dominio de la BrNN parecen propiedad de ésta, ocultando la topología del dominio de la BrNN a la red troncal y reduciendo el número de lugares de difusión en ésta.

Una función BrNN presenta una interfaz de nodo de red convencional sobre los enlaces hacia abajo. Los nodos finales del dominio de la función BrNN registran sus recursos en dicha función y la usan como servidor de nodos de red convencional.

Una BrNN:

- Reduce el número de nodos de red en una red APPN grande.
- Tiene una topología de filial que está oculta a la WAN y una topología de WAN que está oculta a la BrNN.
- Tiene una comunicación directa, de igual a igual, entre ramas conectadas definidas en la misma red de conexiones.
- Reduce el tráfico de sesión de CP-CP en el enlace de la WAN.

Las limitaciones de Branch Extender son:

- Los nodos de red sólo pueden conectarse sobre enlaces que la función BrNN ha definido como enlaces hacia arriba.
- Sólo los nodos finales o las BrNN en cascada pueden conectarse a un enlace hacia abajo de BrNN. Los nodos de frontera que actúan como nodos finales y los nodos del DLUR no pueden conectarse a un enlace hacia abajo de BrNN.
- Un nodo no puede conectarse a Branch Extender sobre un enlace hacia arriba y un enlace hacia abajo al mismo tiempo.
- Una función BrNN puede tener sesiones de CP-CP únicamente con un nodo de red a la vez.

Es posible configurar dos o más funciones BrNN como iguales en una única rama, cada una de las cuales servirá a un conjunto de EN de la rama. Cuando una de estas funciones BrNN pierde conectividad con el servidor de nodos de red preferido, es conveniente que la otra función BrNN se encargue de servir los EN de la primera función BrNN.

Se pueden configurar BrNN de igual a igual de modo que se apoyen automáticamente en esta situación conmutando de una configuración de BrNN de igual a igual a una configuración en cascada.

Extended Border Nodes

Los Extended Border Nodes (BN) permiten que las redes con ID de red diferente se conecten entre sí. Las sesiones de CP-CP se establecen a través de los límites de la red y se permite que los flujos de servicios de directorio y el establecimiento de sesión se amplíen a las redes interconectadas. La información de topología no se intercambia a través del límite de la red. Esto permite que las redes con ID de red diferente establezcan sesiones de CP-CP y al mismo tiempo se proporciona aislamiento topológico entre las diferentes redes.

Además de permitir que las redes con diferentes ID de red se interconecten, los BN proporcionan un mecanismo que sirve para subdividir las redes con el mismo ID en "subredes de topología" más pequeña. Esta subdivisión proporciona aislamiento topológico entre las dos subredes y, además, permite que las sesiones y los flujos de servicios de directorio atraviesen los límites de la subred.

Para poder utilizar esta función, es preciso que haya un BN en un lado del límite de la subred. Cuando un BN se conecta con un NN no nativo, el BN parecerá un EN al NN mencionado, incluso aunque el BN sea, en realidad, un NN.

Pueden haber dos BN, uno a cada lado del límite, cooperando para aplicar esta función. Cuando dos BN se conectan a través del límite de la red, el BN parecerá un NN al BN no nativo.

Un BN parecerá un servidor de NN para todos los recursos no nativos a los que se pueda acceder a través de BN. Esto permitirá que las funciones de cálculo de ruta y puesta en antememoria de directorios de APPN trabajen, además de habilitar al BN para que intercepte y modifique todos los flujos Locate (de localización) y BIND que crucen un TG intersubredes (ISTG).

Los BN implementan el cálculo de ruta de sesión óptimo por partes inteligentes. Cada subred calcula su propia parte del vector de control de la selección de ruta (RSCV) hasta el punto de entrada a la siguiente subred no nativa. Aunque el RSCV sea óptimo en la subred nativa, no hay garantía de que la ruta de la sesión de extremo a extremo sea óptima.

Ejemplo de topología de red

La Figura 1 en la página 18 muestra varias de las opciones de conectividad que proporciona la función BN. Por lo general, puede ir de cualquier red a cualquier red salvo que Red F sólo puede llegar a la red Red E y Red E es la única red que puede llegar a Red F.

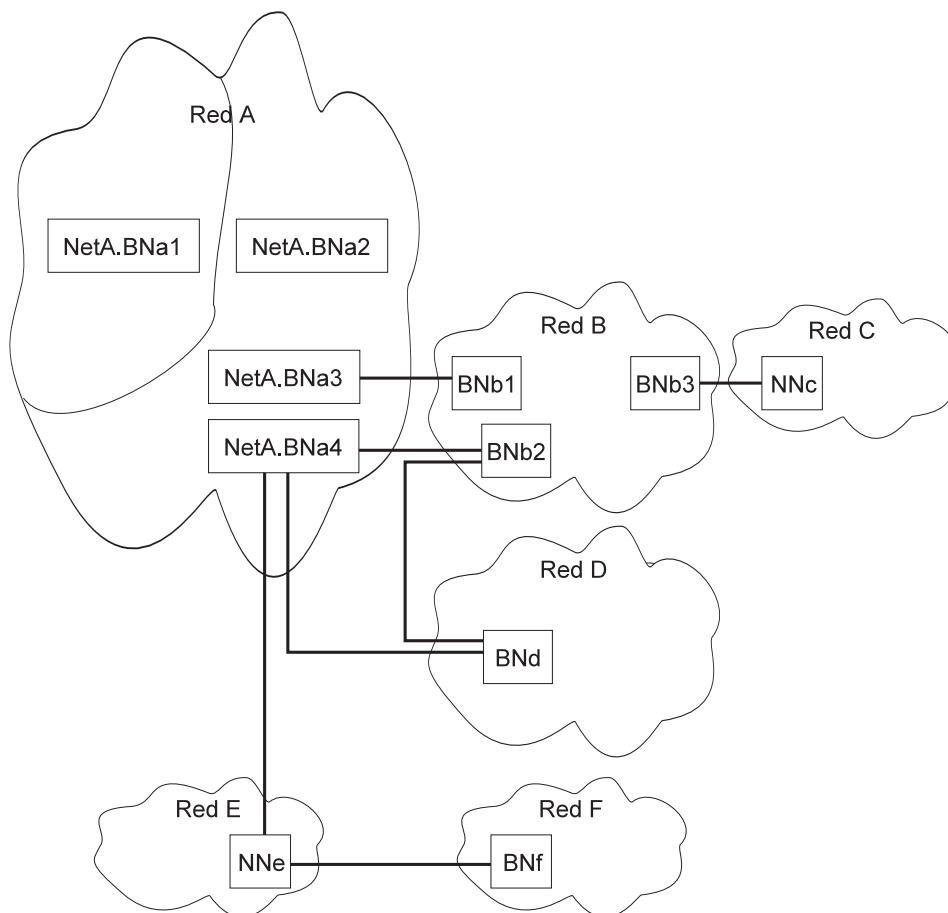


Figura 1. Conectividad de Extended Border Node

Nota: Las líneas en negrita representan los TG intersubred.

En esta figura:

- El Idred de la subred Red A se ha dividido en subredes topológicas. La subred topológica situada más a la izquierda contiene BNa1, subred que, a su vez, está conectada mediante un TG intersubred a BNa2 en la subred topológica de la derecha. El idred de BNa1 y BNa2 es Red A.
- BNa1 no es nativa para el resto de los nodos de frontera ampliado, incluyendo NetA2.
- BNa2, BNa3 y BNa4 son nativas para la subred topológica derecha de Red A, y no son nativas para el resto de las redes, incluyendo la subred que contiene BNa1.
- Un BN puede establecer conexiones con varias redes como es el caso de BNa4, que conecta la subred topológica de Red A con Red B y Red D.
- Dos redes pueden conectarse con varios enlaces como es el caso de la subred topológica derecha de Red A y de Red B, que están conectados por BNa3/BNb1 y BNa4/BNb2.
- Los dos extremos de un enlace entre redes deben ser BN, a menos que una de las redes sea periférica. En dicho caso, esta última red deberá usar un nodo de red no BN convencional para conectarse con el BN de la red adya-

cente. En el ejemplo se ve dónde la red periférica Red C se conecta con Red B mediante NNc.

- Cualquier LU de las subredes Red A, Red B, Red C, Red D o Red E puede llegar a cualquier LU de cualquiera de las redes. Tanto Red C como Red E están conectadas con nodos de red no BN convencionales.
- La red Red E está conectada con el nodo de red NNe no BN convencional a los BN de NetA2 y Red F. Un nodo de red no puede interconectar redes no periféricas, por lo que no se puede ir de Red F a ninguna otra red, salvo Red E.
- Puede ir de NetA2 a Red E y de Red E a NetA2 ya que NNe está en una red periférica. Asimismo, puede ir de Red F a Red E y viceversa.

Extensiones de servicios de sesión (SSE) para soporte NNS

La función SSE de un direccionador se habilita cuando se habilita el direccionador para APPN. Esto es cierto incluso si la función Extended Border Node no está habilitada; lo que significa que el direccionador debe actuar como servidor de nodos de red para un nodo final VTAM. Como tal, puede manejar funciones NNS para nodos finales que soliciten sesiones iniciadas por SLU, sesiones iniciadas por terceros, puesta en cola de peticiones de sesión, inicio de sesión automático, peticiones de liberación de sesión y registro de vectores EN TG.

La función SSE no se usa cuando el direccionador actúa como Branch Extender ya que los VTAM de nivel inferior no están permitidos en dicha configuración.

Requisitos de red

No se requieren otros nodos APPN en una red, siempre y cuando estos nodos no estén conectados directamente a un BN a través del límite topológico. Los nodos APPN conectados a un BN a través de un límite topológico (mediante un ISTG) deben cumplir uno de los requisitos siguientes:

- APPN Ver1 con el conjunto de opciones 1013, posibilidad de funcionar con nodos de frontera ampliado periféricos
- APPN Ver2, donde el conjunto de opciones 1013 forma parte del software básico.

Los nodos conectados usando ISTG que no cumplan alguno de estos dos requisitos generarán alertas y no manejarán algunos de los flujos nuevos asociados al BN. No obstante, si hay otras vías de acceso disponibles en la red, es posible que pueda seguir teniendo conectividad de extremo a extremo.

Comparación de Branch Extender con Extended Border Node

Tanto Branch Extender como Extended Border Nodes sirven para minimizar la topología de la red. La elección de una de estas dos opciones dependerá de la red.

Branch Extender es la opción adecuada cuando se tiene una única red con uno o varios grupos de nodos finales, donde cada grupo de nodos necesita normalmente comunicarse con otros nodos finales del grupo y sólo, en contadas ocasiones, tiene la necesidad de operar con la red troncal.

Ninguno de los dispositivos en sentido directo de Branch Extender puede ser un nodo de red, un DLUR, VTAM o un nodo final de VTAM.

Con Branch Extender, la vista que tendrá la red troncal de éste consistirá en un nodo final gigante con todas las LU en sentido directo que son propiedad de este nodo final. La red troncal no sabrá cuál es la topología en sentido directo de Branch Extender, por lo que se reducirá la sobrecarga de intercambios topológicos. Por el contrario, el servidor de nodos de la red de Branch Extender, que forma parte de la red troncal, sabrá cuáles son todas las LU que son propiedad de dicha función si ésta está configurada para registrar recursos. Esto sirve para reducir el número y tamaño de las difusiones de búsquedas y de actualizaciones topológicas.

Un **nodo de frontera ampliado** (Extended Border Node) es la opción adecuada cuando se desea unir varias redes o bien cuando se tiene una red grande que se desea subdividir, sin que haya restricción alguna sobre los tipos de nodos permitidos en las partes subdivididas. No existe el concepto de sentido inverso o sentido directo y se pueden tener nodos de frontera ampliado, nodos de red, nodos finales, nodos de DLUR, VTAM o finales VTAM adicionales situados en cualquier lugar de la red. A diferencia de Branch Extender, un nodo de frontera ampliado no puede registrar recursos en otra red.

Gestión de un nodo de red

El nodo de red del direccionador puede actuar como un punto de entrada de APPN que reenvía alertas relacionadas con APPN a un punto focal de APPN. Los puntos focales de APPN pueden definirse explícita o implícitamente.

Puede usar SNMP para acceder a estas MIB estandarizadas de IETF:

- APPC (RFC 2051)
- APPN (RFC 2155)
- HPR (RFC 2238)
- DLUR (RFC 2232)
- Extended Border Node
- TN3270 Base
- TN3270 Response Time

También puede usar SNMP para acceder a estas MIB específicas de empresa:

- IBM APPN Memory
- IBM Accounting
- IBM HPR NCL
- IBM HPR Route Test
- IBM Branch Extender Node
- IBM TN3270 Connection Rejection

Posibilidades del punto de entrada para alertas relacionadas con APPN

El nodo de red del direccionador puede servir como punto de entrada de APPN para las alertas relacionadas con el protocolo APPN. En su calidad de punto de entrada, el direccionador es responsable de reenviar alertas genéricas de LU 6.2 y APPN acerca de sí mismo y de los recursos de su dominio a un *punto focal* para su proceso centralizado. Un punto focal es un punto de entrada que proporciona gestión centralizada y control a otros puntos de entrada para una o varias categorías de gestión de red.

Nota: Si un punto focal no está disponible para recibir una alerta de un dispositivo, éste la retendrá (almacenará).

Los puntos de entrada que se comunican con un punto focal forman la *esfera de control* de dicho punto. Si un punto focal define explícitamente los puntos de entrada de su esfera de control e inicia la comunicación con dichos puntos, se tratará de un *punto focal explícito*. Si los puntos de entrada designan un punto focal e inician la comunicación con éste, se tratará de un *punto focal implícito*. El punto focal del direccionador puede ser implícito o explícito.

Los direccionadores configurados como nodos de Branch Extender tienen una flexibilidad adicional. Como ocurre con los nodos de red convencionales, el punto focal puede establecer directamente una relación explícita con el nodo de Branch Extender. Además, como también ocurre en dicho caso, se pueden configurar uno o varios puntos focales implícitos en este nodo.

A diferencia de los nodos de red convencionales, los nodos de Branch Extender también pueden utilizar el servidor de nodos de la red para adquirir conocimientos sobre su punto focal. Cuando el servidor de nodos de red establece una relación con el punto focal, ya sea explícita o implícitamente, notifica a todos los nodos finales a los que sirve, incluyendo los nodos de Branch Extender, el nombre del punto focal.

Si la sesión entre el punto de entrada del direccionador y el punto focal primario falla, el direccionador podrá iniciar una sesión con un punto focal de reserva designado. Antes de iniciar una sesión con el mencionado punto focal, el punto de entrada del direccionador intentará volver a establecer la comunicación con el punto focal primario si se ha asignado al direccionador la responsabilidad de restablecimiento de sesión. Si el intento falla, el direccionador pasará al punto focal de seguridad.

Nota: El direccionador intentará establecer una sesión con el punto focal de seguridad o intentará volver a establecer la sesión con el punto focal primario, únicamente si tiene que enviar una alerta.

Después de pasar al punto focal de seguridad, el direccionador intentará periódicamente volver a establecer sesión con el punto focal primario. El intervalo entre intentos se duplicará cada vez que falle un intento, hasta alcanzar un intervalo máximo de un día. A partir de ese momento, el intento se efectuará cada día.

Notas:

1. Si el punto focal es explícito y el punto focal explícito guarda para sí mismo la responsabilidad de restablecimiento, este mecanismo de reintento quedará inhabilitado.
2. Si el punto focal es explícito y asigna responsabilidades de restablecimiento al direccionador, éste intentará volver a establecer la comunicación hasta el siguiente reinicio de APPN en el direccionador.

El punto de entrada del direccionador se comunica con el punto focal mediante una sesión LU 6.2. El soporte de diversos dominios (MDS) es el mecanismo que controla el transporte de las peticiones de servicios de gestión y los datos entre estos nodos. El nodo de red del direccionador *no* da soporte a las sesiones de SSCP-PU con los puntos focales.

Los procesos de gestión del punto de control del direccionador están gestionados por el componente de los servicios de gestión del punto de control (CPMS). El componente CPMS del nodo de red del direccionador recoge datos de gestión de problemas no solicitados en los recursos del dominio del direccionador y los reenvía al punto focal adecuado.

Unidades de mensaje con soporte

El nodo de red del direccionador usa las unidades de mensaje siguientes para enviar y recibir datos de servicios de gestión, incluyendo mensajes de alerta de EN de dominio:

Unidad de mensaje Descripción

CP-MSU	Unidad de servicios de gestión del punto de control. Esta unidad de mensaje está generada por CPMS y contiene información de alerta reenviada por el punto de entrada del direccionador. CPMS pasa unidades de mensaje CP-MSU a MDS.
MDS-MU	Unidad de mensaje de soporte de diversos dominios. Esta unidad de mensaje está generada por MDS. Éste encapsula CP-MSU para efectuar el transporte entre nodos.

Posibilidades SNMP para las MIB de APPN

Un operador o una aplicación de una estación de gestión de red SNMP puede solicitar objetos en las MIB de APPN (usando los mandatos de SNMP **get** y **get_next**) para recuperar información de estado de APPN y estadísticas de nodos. También puede modificar un subconjunto de objetos de MIB de APPN usando el mandato **set** de SNMP. Sólo se puede acceder a las MIB de APPN a través de SNMP.

Recogida de desechos (Garbage Collection) de la base de datos de topología

La información fluye entre los NN de APPN para informar a los mismos sobre los recursos de la red. Cada NN mantiene una base de datos de topología formada por los nombres y características de dichos recursos. Cuando se elimina un recurso de la red, también puede eliminarse de cada base de datos de topología de NN. Cuando un NN detecta que un recurso de su base de datos de topología ha quedado obsoleto, el nodo difundirá información en la que indicará que el recurso deberá enviarse a la basura. Si los NN que reciben esta información dan soporte a Enhanced Garbage Collection, deberán suprimir el recurso de su base de datos de topología. En realidad, el registro no será recogido para desecharlo hasta el siguiente ciclo de recogida de desechos. Un NN examina cada uno de los recursos de su base de datos de topología, todos los días.

Cola de alertas retenidas configurable

La función de cola de alertas retenidas configurable le permite configurar el tamaño de la mencionada cola. Si no hay ningún punto focal disponible, la cola de alertas retenidas guardará las alertas de APPN. Cuando vuelva a haber un punto focal disponible, se enviarán las alertas retenidas. Si llegan más alertas de las que se pueden guardar, se descartarán las de mayor antigüedad.

Nota: Si configura un valor grande para Held Alert Queue Size (tamaño de la cola de alertas retenidas), deberá tener en cuenta la memoria adicional. Podrá hacerlo dejando que el algoritmo de ajuste calcule automáticamente el valor Maximum Shared Memory (memoria compartida máxima). Consulte "Ajuste

del nodo APPN” en la página 40 para obtener información adicional acerca del algoritmo de ajuste de nodos.

Punto focal implícito

Un punto focal es un nodo responsable de la gestión centralizada. El nodo de gestión puede ponerse en contacto con el nodo gestionado (direccionador) y establecer una sesión de gestión. El nodo de gestión será, por lo tanto, un punto focal explícito. Cuando el nombre del nodo de gestión se configura en el direccionador y éste puede iniciar una sesión de gestión, el nodo de gestión será un punto focal implícito. Puede configurar un punto focal único implícito primario que tenga hasta ocho puntos focales implícitos de seguridad, donde cada punto focal sea un nombre de red plenamente calificado. El direccionador intentará ponerse en contacto con cada punto focal siguiendo un orden, hasta establecer una sesión de gestión satisfactoria.

Si la sesión de gestión se ha establecido con un punto focal implícito de seguridad, el dispositivo intentará, periódicamente, volver a establecer sesión con el punto focal implícito primario. El intervalo entre intentos se duplicará cada vez que falle un intento, hasta alcanzar un intervalo máximo de un día. A partir de ese momento, el intento se efectuará cada día.

Nota: Si un punto focal explícito inicia una sesión de gestión de un dispositivo, hará que una sesión con un punto focal implícito termine.

Soporte de Enterprise Extender para HPR sobre IP

El soporte de Enterprise Extender para HPR sobre IP permite que las aplicaciones HPR/APPN se ejecuten sobre una red troncal IP y sigan aprovechando el tipo de servicio de APPN. HPR sobre IP encapsula datos HPR en un paquete UDP/IP para entregar en la red IP.

DLC con soporte

La Tabla 2 muestra los puertos de DLC que tienen soporte del dispositivo sobre APPN:

Tabla 2 (Página 1 de 2). Tipos de puerto con soporte para direccionamiento de APPN

Tipo de puerto	Estándar	HPR	ISR	DLUR ¹
Ethernet	Versión 2	Sí	Sí	Sí
Ethernet	IEEE 802.3	Sí	Sí	Sí
TR	802.5	Sí	Sí	Sí
PPP en serie		Sí	Sí	No
FR en serie (puenteado y direccionado) ²		Sí	Sí	Sí
Frame Relay BAN		Sí	Sí	Sí
Puenteo de LAN en serie		ND	ND	ND
SDLC		No	Sí	Sí
X.25	CCITT X.25	No	Sí	Sí
DLSw		No	Sí	Sí

Tabla 2 (Página 2 de 2). Tipos de puerto con soporte para direccionamiento de APPN

Tipo de puerto	Estándar	HPR	ISR	DLUR ¹
APPN/PPP/RDSI		Sí	Sí	No
APPN/FR/RDSI		Sí	Sí	Sí
APPN/PPP/V.25 bis		Sí	Sí	No
APPN/PPP/V.34		Sí	Sí	No
LANE	Se ajusta al Forum	Sí	Sí	Sí
ATM		Sí	No	Sí
HPR sobre IP		Sí	No	Sí
100Mbps Ethernet		Sí	Sí	Sí
100Mbps TR	802.5	Sí	Sí	Sí

Proceso de configuración del direccionador

En esta sección se describe el proceso de configuración del direccionador y se incluyen detalles acerca de los parámetros.

Cambios en la configuración que necesitan un reinicio de la función APPN

- ID de red del nodo de red
- Nombre de punto de control del nodo de red
- Número XID (de nodo de red) para la conexión de subárea
- Tipo de nodo adyacente (de estación de enlace)
- Cambio de la función de nodo (EBN, BN, NN)
- Cualquier parámetro que esté bajo las opciones siguientes:
 - Direccionamiento de alto rendimiento (HPR) en el nivel de nodo
 - Peticionario de LU dependientes (DLUR) en el nivel de nodo
 - Red de conexiones
 - Clase de servicio
 - Ajuste de nodo
 - Gestión de nodo
 - Puntos focales
 - Correlaciones de nombres de modalidades
 - Parámetros de supresión de TN3270E
 - Listas de direccionamientos
 - Tablas de correlaciones de CoS

Consulte la sección “Soporte de reconfiguración dinámica de APPN” en la página 283 si desea obtener información acerca de los cambios dinámicos que se pueden efectuar en la configuración de APPN.

¹ Esta columna hace referencia al puerto que proporciona la conexión con la PU en sentido directo (DSPU).

² Utilice el formato puentado cuando tenga dos dispositivos conectados por Frame Relay y uno de ellos no tenga APPN. De lo contrario, utilice el formato direccionado debido a su mejor rendimiento.

Requisitos de configuración de APPN

El direccionamiento de APPN se configura en adaptadores individuales que dan soporte al DLC deseado. Para usar el direccionamiento de APPN, debe estar configurado y habilitado, como mínimo, uno de los DLC siguientes:

- Puertos de LAN:
 - Red en anillo
 - Ethernet
- Puertos serie configurados con:
 - PPP
 - Frame relay
 - X.25
 - SDLC
 - Circuitos de marcación sobre RDSI
 - Circuitos de marcación sobre V.25 bis
 - Circuitos de marcación sobre V.34
- DLSw
- ATM
- HPR sobre IP

Configuración del direccionador como nodo de red de APPN

Puede configurar el direccionador como nodo de red APPN de tres maneras diferentes, según el nivel de conectividad deseado con el resto de los nodos.

- Configuración mínima
- Configuración de inicio de conexiones
- Configuración de control de conexiones

Configuración mínima

Este grupo de pasos de configuración de APPN:

- Permite que el nodo de red acepte cualquier solicitud que reciba de otro nodo para establecer conexión.
- Evita que el nodo de red inicie conexiones con otros nodos.

Si elige la configuración mínima, los nodos adyacentes deberán definir conexiones con el nodo de red del direccionador para asegurar la conectividad. Dado que los nodos APPN pueden iniciar sesiones de CP-CP con el nodo de red del direccionador, no es necesario definir estos nodos en la configuración del direccionador. Por lo general, cuando configure APPN en el direccionador, podrá simplificar en gran medida esta tarea si permite que el nodo de red del direccionador acepte solicitudes de conexión de cualquier nodo. Si configura el nodo de red de esta manera, no tendrá que definir información sobre los nodos adyacentes, salvo en los casos siguientes:

- El nodo adyacente es un nodo final LEN. Los nodos finales LEN no dan soporte a las sesiones de CP-CP, por lo que la información sobre dichos nodos y sus recursos LU debe configurarse en el nodo de red del direccionador.
- Quiere que el nodo de red del direccionador pueda iniciar una sesión de CP-CP con un nodo APPN adyacente.

En dichos casos, debe especificar información sobre el nodo adyacente cuando habilite el direccionamiento de APPN en el puerto específico que está usando para conectarse con el mencionado nodo y debe seguir los pasos de configuración descritos en “Configuración de inicio de conexiones” en la página 26.

Use el procedimiento siguiente para los pasos de configuración mínima:

1. Si está configurando APPN usando un puerto DLSw:
 - a. Habilite el puenteo en el nodo
 - b. Habilite DLSw en el nodo
 - c. Defina el puerto de DLSw con una dirección del MAC administrada localmente para DLSw.
2. Habilite el direccionamiento de APPN en el puerto.

Nota: Debido a que Service Any (servir a cualquiera) está habilitado por omisión, el nodo aceptará cualquier solicitud de conexión que reciba de otro nodo.
3. Habilite el nodo de red APPN.
4. Configure los parámetros siguientes:
 - Network ID (ID de red)
 - Control point name (Nombre del punto de control)
5. Defina el número XID del parámetro de conexiones de subárea para el nodo de red APPN (opcional).
6. Acepte el resto de valores por omisión.
7. Opcionalmente lleve a cabo las acciones siguientes:
 - Modifique los parámetros del direccionamiento de alto rendimiento
 - Configure el peticionario de LU dependientes
 - Defina redes de conexiones
 - Defina nuevas correlaciones de nombres de modalidades y de nombres de CoS
 - Ajuste el rendimiento de este nodo
 - Ejecute diagnósticos de rastreo de servicios de nodo
 - Recoja estadísticas para este nodo de red

Notas:

1. El direccionamiento de APPN debe estar definido y habilitado en los puertos específicos cuya utilización haya configurado en el nodo de red del direccionador.
2. El puenteo y DLSw deben seguir estando habilitados en los puertos de los adaptadores específicos que desee que el nodo de red del dispositivo use.

Configuración de inicio de conexiones

Este grupo de pasos de configuración de APPN:

- Permite que el nodo de red acepte cualquier solicitud que reciba de otro nodo para establecer conexión.
- Habilita al nodo de red para que inicie conexiones con los nodos que especifique, incluyendo los nodos finales LEN.

Dado que los nodos APPN pueden iniciar sesiones de CP-CP con el nodo de red del direccionador, no es necesario definir estos nodos en la configuración del direccionador, salvo en los casos siguientes:

- El nodo adyacente es un nodo final LEN. Los nodos finales LEN no dan soporte a las sesiones de CP-CP, por lo que la información sobre dichos nodos y sus recursos LU debe configurarse en el nodo de red del direccionador.
- Quiere que el nodo de red del direccionador pueda iniciar una sesión de CP-CP con un nodo APPN adyacente.

Si ninguno de estos casos se puede aplicar a la configuración, siga los pasos de configuración descritos en “Configuración mínima” en la página 25.

Siga el procedimiento siguiente para la configuración de inicio de conexiones:

1. Si está configurando APPN usando un puerto DLSw:
 - a. Habilite el puenteo en el nodo
 - b. Habilite DLSw en el nodo
 - c. Defina el puerto de DLSw con una dirección del MAC administrada localmente para DLSw.
2. Seleccione los puertos sobre los que iniciará conexiones con los nodos adyacentes. A continuación, se muestran los tipos de puerto de DLC que tienen soporte de APPN:
 - Puerto de LAN en anillo
 - Puerto de LAN Ethernet
 - Puerto serie Frame-relay
 - Puerto serie PPP
 - X.25
 - SDLC
 - DLSw
 - Puerto IP
3. Habilite el direccionamiento APPN en los puertos APPN con el parámetro *enable APPN routing on this port* (habilitación del direccionamiento APPN en este puerto).

Nota: Debido a que Service Any (servir a cualquiera) está habilitado por omisión, el nodo aceptará cualquier solicitud de conexión que reciba de otro nodo.
4. Defina las estaciones de enlace de APPN en los puertos de DLC seleccionados para los nodos adyacentes con los que este nodo de red puede iniciar conexión.

Nota: No es necesario definir las estaciones de enlace en todos los puertos, únicamente en aquellos sobre los que desee iniciar conexiones con nodos adyacentes.
5. Habilite el nodo de red APPN.
6. Configure los parámetros siguientes para el nodo de red APPN:
 - a. Network ID (ID de red)
 - b. Control point name (Nombre del punto de control)

7. Defina el número XID del parámetro de conexiones de subárea para el nodo de red APPN (opcional).
8. Acepte el resto de valores por omisión.
9. Opcionalmente lleve a cabo las acciones siguientes:
 - Modifique los parámetros del direccionamiento de alto rendimiento
 - Configure el peticionario de LU dependientes
 - Defina redes de conexiones
 - Defina nuevas correlaciones de nombres de modalidades y de nombres de CoS
 - Ajuste el rendimiento de este nodo
 - Ejecute diagnósticos de rastreo de servicios de nodo
 - Recoja estadísticas para este nodo de red

Configuración de control de las conexiones

Este grupo de pasos de configuración de APPN:

- Permite que el nodo de red acepte sólo las solicitudes de aquellos nodos que especifique.
- Habilita al nodo de red para que inicie conexiones con los nodos que especifique, incluyendo los nodos finales LEN.

Esta configuración aporta un mayor nivel de seguridad ya que se define explícitamente qué nodos APPN podrán comunicarse con el nodo de red del direccionador. Sólo se aceptará una solicitud de conexión de un nodo adyacente si el parámetro del nombre del CP plenamente calificado se ha configurado en este nodo de red. Este grupo de pasos de configuración le habilita opcionalmente para tener un enlace seguro con cada nodo adyacente configurando la función de seguridad de nivel de sesión para cada enlace.

Siga el procedimiento siguiente para configurar el control de las conexiones:

1. Seleccione los puertos sobre los que desee establecer conexiones con nodos adyacentes desde los tipos de puertos de DLC siguientes con soporte de APPN:
 - Puerto de LAN en anillo
 - Puerto de LAN Ethernet
 - Puerto serie Frame-relay
 - Puerto serie PPP
 - X.25
 - DLSw
 - SDLC
 - Puerto IP
2. Defina los puertos seleccionados como puertos APPN directos con los parámetros siguientes:
 - Habilite *APPN routing* (direccionamiento APPN) en este puerto
 - Inhabilite el parámetro Service any port (servir cualquier puerto)
3. Si está configurando APPN usando un puerto DLSw:
 - Habilite el puenteo en el nodo
 - Habilite DLSw en el nodo.
 - Defina los puertos de DLSw con el parámetro siguiente:
 - Defina una dirección del MAC administrada localmente para DLSw

- Inhabilite el parámetro Service any node (servir cualquier nodo)
4. Habilite el direccionamiento de APPN en el puerto.
 5. Defina las estaciones de enlace de APPN en los puertos de DLC seleccionados para los nodos adyacentes:
 - que pueden iniciar una conexión con este nodo de red.
 - con los que desea que este nodo de red de direccionador inicie una conexión.

Especifique los parámetros de estación de enlace siguientes:

 - Fully Qualified CP name of adjacent node (Nombre del CP plenamente calificado del nodo adyacente) (obligatorio)
 - Cualquier parámetro de direccionamiento necesario para el nodo adyacente
 - Y, opcionalmente:
 - CP-CP Session Level Security (Seguridad del nivel de sesión de CP-CP)
 - Security Encryption Key (Clave de codificación de la seguridad)
 6. Habilite el nodo de red APPN.
 7. Configure los parámetros siguientes para el nodo de red APPN:
 - Network ID (ID de red)
 - Control point name (Nombre del punto de control)
 8. Defina el número XID del parámetro de conexiones de subárea para el nodo de red APPN (opcional):
 9. Acepte el resto de valores por omisión.
 10. (Opcional) Configure las opciones del nodo de red del direccionador siguientes:
 - Modifique los parámetros del direccionamiento de alto rendimiento
 - Configure el petionario de LU dependientes
 - Defina redes de conexiones
 - Defina nuevas correlaciones de nombres de modalidades y de nombres de CoS
 - Ajuste el rendimiento de este nodo
 - Ejecute diagnósticos de rastreo de servicios de nodo
 - Recoja estadísticas para este nodo de red

Configuración de Branch Extender

Para configurar Branch Extender, establezca los parámetros de configuración siguientes como considere adecuado para la red.

1. Utilice el mandato **set node** para:
 - a. Responder 1 para elegir Branch Extender cuando se le pregunte Enable Branch Extender or Border Node (habilitar Branch Extender o Border Node). Si responde 0, no aparecerá ninguna de las preguntas de Branch Extender.
 - b. Responder Full (completo), Partial (parcial) o None (ninguno) a la pregunta *Enable Branch Awareness Support* (habilitar el soporte de Branch Awareness), dependiendo de si desea limitar el flujo de información de topología acerca de los TG entre NN y BrNN.

- c. Responder yes (sí) o no a la pregunta Permit search for unregistered LUs (Permitir búsqueda de LU no registradas) según si desea permitir o no búsquedas desde la red troncal de LU que no se registraron en el servidor de nodos de red.
 - d. La respuesta a la pregunta Branch uplink (enlace hacia arriba de la rama) determinará el valor por omisión de la pregunta análoga del nivel de enlace.
2. Use el mandato **add link** para:
- a. Responder sí a la pregunta *Branch uplink* si desea que el direccionador aparezca como nodo final en este enlace. Un nodo final es para enlaces con los nodos de red de la red troncal. Tenga en cuenta que esta pregunta no aparece y su valor será sí, si ha definido la estación de enlace adyacente para que sea un nodo de red en uno de los indicadores de configuración anteriores. Responda no si desea que el direccionador aparezca como nodo de red en este enlace. Un nodo de red es para enlaces con nodos finales.
 - b. La pregunta *Is uplink to another Branch Extender node* (Es enlace hacia arriba con otro nodo de Branch Extender) se efectúa sólo si este enlace se ha definido como recurso limitado y también como enlace hacia arriba de Branch Extender. Responda sí si el nodo adyacente es otro Branch Extender.
 - c. La pregunta *Preferred network node server* (servidor de nodos de red preferido) se efectúa sólo si el nodo adyacente es un nodo de red y las sesiones de CP-CP tienen soporte en este enlace. Dado que sólo puede tener un único servidor de nodos de red preferido, esta pregunta no volverá a aparecer una vez haya respondido sí en algún enlace.

Configuración de Extended Border Nodes

Para configurar nodos de frontera ampliado, deberá configurar uno o varios de los parámetros siguientes:

- Set node (Establecer nodo)
- Add port (Añadir puerto)
- Add link (Añadir enlace)
- Add routing_list (Añadir lista_direccionamientos)
- Add cos_mapping_table (Añadir tabla_correlaciones_cos)

Set node

El indicador que existía anteriormente y se usaba para habilitar Branch Extender se ha ampliado para poder elegir la función de Branch Extender, la de Extended Border Node o ninguna. Únicamente si habilita la función Extended Border Node aparecerán otros indicadores de nodo de frontera ampliado.

Subnetwork visit count (recuento de visitas a la subred) es el primer indicador. Este parámetro define el número máximo de subredes topológicas que puede atravesar una sesión. El valor indicado se usará como valor por omisión para el nodo de frontera ampliado. Se pueden especificar valores diferentes para el recuento de visitas a la subred al añadir puertos, enlaces o listas de direccionamientos.

Cache search time (Tiempo de búsqueda en la antememoria) es el indicador de nivel del nodo siguiente. Este parámetro especifica el tiempo en minutos durante el cual el nodo de frontera ampliado mantendrá información en las búsquedas efec-

tuadas en varias subredes. El objetivo es que este parámetro sirva de mecanismo primario para limitar el tamaño de la antememoria. No obstante, el parámetro siguiente también se puede usar para controlar dicho tamaño.

Maximum search cache size (tamaño máximo de la antememoria de búsqueda) es el parámetro siguiente. Este parámetro controla la misma estructura de datos controlada por el parámetro anterior. Si se establece en cero, el tamaño máximo será ilimitado. Sólo se descartarán las entradas después de que haya vencido el plazo de la antememoria de búsqueda. Si prefiere que el tamaño máximo de la antememoria sea fijo, especifíquelo aquí. Si el máximo se alcanza antes de que alguna entrada supere el límite de tiempo, se descartarán las entradas menos recientes.

List dynamics (Listar dinámica) es el indicador siguiente y permite controlar el modo en que el nodo de frontera ampliado determina los saltos siguientes posibles al intentar localizar recursos (LU). El código operativo crea dinámicamente la lista temporal de los posibles CP del salto siguiente siempre que el nodo intenta localizar un recurso. Este parámetro especifica las fuentes de los nombres de CP del salto siguiente que puede usar el nodo de frontera ampliado para crear esta lista dinámica temporal de nombres de CP.

Después de crear la lista temporal, ésta siempre se ordena de tal modo que los CP de salto siguiente configurados van seguidos primero de los CP asociados con recursos conocidos que tienen nombres similares. Puede efectuarse un cambio de orden adicional. Una vez finalizado el cambio de orden, el nodo de frontera ampliado empezará a buscar el recurso deseado en un CP tras otro.

Tenga en cuenta que una vez el nodo de frontera ampliado haya localizado un recurso, el nodo recordará cuál es el CP del salto siguiente y siempre usará el CP de dicho salto para el mencionado recurso, sin tener en cuenta las listas de direccionamientos. Las entradas de esta tabla de recursos localizados pueden durar bastante tiempo. Se descartarán si la tabla alcanza su tamaño máximo, una búsqueda posterior en el CP no consigue localizar el recurso o si la búsqueda de la LU proviene de un CP diferente.

El parámetro list dynamics (listar dinámica) se establece en uno de los valores siguientes. Se puede volver a especificar este valor para listas de direccionamientos individuales cuando configure, si configura, listas de direccionamientos individuales.

None (Ninguno) El nombre de LU del recurso de destino se compara con los nombres de LU configurados en las listas de direccionamientos. Se selecciona la lista de direccionamientos que tenga la mejor coincidencia de nombre de LU y los nombres de CP del salto siguiente de la lista configurada se ponen en la lista creada dinámicamente. Esta es la única fuente de nombres de CP de salto siguiente que se tiene cuando list dynamics se establece en none.

Tenga en cuenta que si un nombre de LU no aparece en una lista de direccionamientos, el nodo de frontera ampliado no podrá alcanzarla cuando este parámetro se establezca en none.

Limited (Limitado) Este valor aumenta la lista de nombres de CP de salto siguiente obtenida a partir de la lista de direccionamientos configurada según mejor coincidencia, con nombres de CP obtenidos a partir de los

conocimientos que tiene el nodo de frontera ampliado de los recursos y la topología existentes. Estos nombres de CP adicionales se obtienen:

- Añadiendo todos los nodos de frontera ampliado nativos
- Añadiendo todos los nodos de frontera ampliado adyacentes, no nativos y los nodos de red con IDRED que coincida con el IDRED del recurso de destino.
- Examinando la tabla de recursos que el nodo de frontera ampliado ya conozca debido a la recepción de una variable GDS buscada o encontrada. Estos recursos se ponen en antememoria en la base de datos de servicios del directorio. En el caso de las entradas donde el Idred de la LU en antememoria sea el mismo que el destino de la búsqueda actual, se añade el NN de la LU de la antememoria a la lista de CP de salto siguiente.

Ninguno de estos nombres de CP de salto siguiente obtenidos dinámicamente se guardan permanentemente con los datos de la configuración. La lista se vuelve a crear siempre que es necesario localizar un recurso.

Full (Completo) Este valor funciona igual que el valor Limited (limitado), salvo que se elimina la restricción sobre los IDRED coincidentes cuando se añaden todos los nodos de frontera ampliado adyacentes no nativos y los nodos de red.

Si se habilita *list optimization* (Optimización de lista), el proceso de reordenamiento que se describe en la página 31 se repetirá otra vez y los nombres de CP obtenidos a partir de los datos configurados también podrán volver a ordenarse.

Si se habilita *load balance* (equilibrio de carga) a través de los límites entre subredes paralelas, el direccionador intentará equilibrar el número de sesiones entre dos o más puntos de salida entre subredes paralelas. La configuración relevante tiene dos o más direccionadores que sirven como puntos de salida EBN en una subred con el mismo número en la otra subred. Cada direccionador tiene un TG entre subredes hacia un direccionador distinto en la otra subred, que forman dos o más enlaces paralelos. (Tenga en cuenta que no se trata de TG paralelos entre cualquier par de direccionadores.)

Para habilitar esta función de equilibrio de carga, es necesario configurar listas de direccionamiento en cada direccionador EBN, de modo que las sesiones para nombres de LU de destino distintos tengan EBN de salida preferibles distintos. También se configurará el límite entre subredes preferible y se podrán establecer recorridos de seguridad.

Add port

Si se habilita el nodo de frontera ampliado, aparecerán dos indicadores adicionales cuando invoque la opción de menú add port (añadir puerto). Estos dos indicadores nuevos establecen el valor por omisión de los parámetros análogos en el nivel de enlace. Los valores de estos parámetros del nivel de enlace determinan el comportamiento de la estación de enlace.

Subnetwork visit count es el primero de estos parámetros y describe el mismo concepto que el definido en el nivel de nodo. Cuando se configura por primera vez un puerto, se inicializa este parámetro en la configuración de nodo. Con este pará-

metro, se permite que los puertos individuales se desvíen de la configuración de nivel de nodo.

El parámetro *Adjacent subnetwork affiliation* (afiliación a la subred adyacente) está controlado por el otro indicador nuevo de nodo de frontera ampliado. Este valor permite que defina si el nodo adyacente está o no en la misma red que el nodo de frontera ampliado. El valor especificado se usará como valor por omisión para todos los enlaces efectuados a través del puerto. Los valores permitidos son:

Native (Nativo) El nodo adyacente está en la misma subred topológica que el nodo de frontera ampliado.

Non-native

(No nativo) El nodo adyacente no forma parte de la subred topológica del nodo de frontera ampliado.

Negotiable

(Negociable) El nodo adyacente puede o no estar en la misma subred topológica según cómo se haya definido el nodo adyacente. El nodo adyacente estará en la misma subred topológica del nodo de frontera ampliado, a menos que la definición de enlace correspondiente al nodo adyacente sea una de las siguientes:

- No nativa
- Negociable y el nodo adyacente tenga un nombre de red diferente
- Negociable y el nodo adyacente haya definido el enlace como no nativo

Add link

Si habilita Extended Border Node, cuando invoque la opción de menú add link (añadir enlace) aparecerán los mismos dos indicadores adicionales que se presentaron anteriormente con add port.

Subnetwork visit count y *adjacent subnetwork affiliation* representan el mismo concepto que el indicado en el nivel de puerto. Se inicializan en la configuración de puerto correspondiente cuando se configura por primera vez un enlace. El valor se cambia en este parámetro si desea que diferentes enlaces tengan valores diferentes incluso aunque estén en el mismo puerto.

Add Routing Lists

Nota: Las listas de direccionamientos no tienen soporte en los modelos 2210 12x.

Una lista de direccionamientos configurada le permite definir de forma explícita uno o varios CP de salto siguiente para uno o varios recursos de destino (LU). Puede usar un carácter comodín "*" al definir nombres de LU para reducir la cantidad de datos configurados. También puede variar algunos de los valores por omisión del nivel de nodo de una lista de direccionamientos determinada.

Puede definir varias listas de direccionamientos. Por lo general, un grupo de LU con requisitos de direccionamiento similares se configura en una única lista de direccionamientos. Los grupos de LU adicionales, cada uno con sus propios requisitos de direccionamiento, se configuran en listas de direccionamientos adicionales.

El número de nombres de LU y de CP usados en las listas de direccionamientos tiene un límite. Los límites pueden variar de acuerdo con el modelo de direccionador que tenga. Consulte la Tabla 38 en la página 211 para obtener infor-

mación detallada sobre el mandato. El límite se ha establecido para poder disfrutar de la mayor flexibilidad posible en los diversos entornos. La capacidad del direccionador para manejar la especificación de varias listas de direccionamientos, cada una de ellas con varios nombres de LU y de CP, está limitada por la disponibilidad de memoria no volátil de configuración, memoria del direccionador y memoria compartida de APPN. Consulte el "Ajuste del nodo APPN" en la página 40 para obtener información sobre los parámetros de ajuste de APPN que controlan la cantidad de memoria compartida.

Recuerde que, tal como se indica en la explicación del indicador de set node, que el código operativo nunca modifica las listas de direccionamientos configuradas. Cuando el nodo de frontera ampliado usa una lista de direccionamientos determinada, copia los nombres de CP del salto siguiente en una lista de direccionamientos temporal. Esta lista de direccionamientos dinámica temporal aumenta con las entradas dinámicas que permite la configuración del parámetro list dynamics. La lista así obtenida es de corta duración y se descarta una vez se encuentra el recurso de destino o la lista se agota.

El parámetro *routing list name* (nombre de la lista de direccionamientos) es el primer indicador que aparece al añadir o modificar una lista de direccionamientos. El código operativo no utiliza este nombre. El objetivo de este parámetro es permitirle identificar una lista de direccionamientos específica si desea modificarla o suprimirla más tarde.

Subnetwork visit count y *list optimization* son los dos indicadores siguientes y representan el mismo concepto que los parámetros análogos definidos en el nivel de nodo. Una lista de direccionamientos nueva inicializa estos valores con los parámetros del nivel de nodo actual. Los valores de las listas de direccionamientos individuales se cambian a medida que las necesidades del usuario así lo dictan.

El siguiente es el indicador o indicadores *Destination LU* (LU de destino). En este parámetro puede configurar como mínimo un recurso de destino y, opcionalmente, más de uno. Puede acabar antes cualquiera de los nombres de FQLU con un carácter comodín "*" posterior para identificar un grupo de LU. No debe incluir un "*" en medio de un nombre de FQLU.

Una de las listas de direccionamientos puede especificar un "*" autónomo como una de las LU de destino. Si se hace así, dicha lista de direccionamientos se conocerá como default routing list (lista de direccionamientos por omisión) y el nodo de frontera ampliado la utilizará para todas las LU de destino que no coincidan mejor con las LU especificadas en el resto de listas de direccionamientos. Esta lista también se usa para buscar LU cuando se indica INAUTHENTIC NETID.

Cuando modifique una lista de direccionamientos existente que tenga varios nombres de LU, el proceso de repasar los nombres de LU puede ser bastante aburrido. Existe un cierto número de teclas de método abreviado definidas para revisar más rápidamente una lista de nombres existente. Estas teclas se definen en la sección donde se da información detallada del mandato de configuración.

Los indicadores *Routing CP* (CP de direccionamiento) forman la parte final de la entrada en una lista de direccionamientos. En este parámetro se indican los nombres de uno o varios CP que pueden saber cómo llegar a la lista configurada de LU. Junto con cada nombre de CP, puede configurar un recuento opcional de

las visitas a la subred. Esto le permitirá especificar un número máximo de subredes que puede atravesar una sesión para CP diferentes.

Además de configurar explícitamente nombres de FQCP, existen un par de palabras clave definidas que se equiparan con el nombre de CP del nodo local, todos los nodos de frontera ampliado nativos, etc. Consulte la sección con información detallada sobre el mandato de configuración si desea obtener más detalles.

Al igual que ocurre con la lista de nombres de LU, están disponibles las mismas teclas de método abreviado para acelerar la revisión de una lista de nombres de CP existente.

Add CoS Mapping Table

Nota: Las tablas de correlaciones de CoS no tienen soporte en los modelos 2210 12x.

La tabla de correlaciones de clases de servicios permite convertir nombres de CoS no nativos en nombres de CoS nativos y viceversa. Las redes no nativas que utilizan los mismos nombres de CoS que la red nativa del nodo de frontera ampliado no necesitan que se defina una tabla de correlaciones de CoS. Si sólo algunos de los nombres de CoS no nativos son diferentes de los nombres de CoS nativos, entonces sólo deberán configurarse en una tabla de correlaciones de CoS aquellos que sean diferentes.

Una tabla de correlaciones de CoS determinada puede aplicarse a una única red no nativa o bien a varias redes no nativas. Puede definir tantas tablas de correlaciones de CoS como sea necesario.

El número de nombres de redes no nativas utilizado en las tablas de correlaciones de CoS tiene un límite. Los límites pueden variar de acuerdo con el modelo de direccionador que tenga. Consulte la Tabla 39 en la página 215 para obtener información detallada sobre el mandato. El límite se ha establecido para poder disfrutar de la mayor flexibilidad posible en los diversos entornos. La capacidad del direccionador para manejar la especificación de varias tablas de correlaciones de CoS, cada una de ellas con varios nombres de redes no nativas y pares de nombres de CoS, está limitada por la disponibilidad de memoria no volátil de configuración, memoria del direccionador y memoria compartida de APPN. Consulte "Ajuste del nodo APPN" en la página 40 para obtener un análisis detallado de los parámetros de ajuste de APPN que controlan la cantidad de memoria compartida.

CoS mapping table name (Nombre de la tabla de correlaciones de CoS) es el primer indicador. Como ocurre con el nombre análogo utilizado para las listas de direccionamientos, el código operativo no usa este parámetro. Su objetivo es permitirle consultar una tabla de correlaciones de CoS específica para que pueda modificarla o suprimirla. Las tablas de correlaciones de CoS diferentes deben tener nombres diferentes, pero una tabla de correlaciones de CoS determinada puede tener un nombre idéntico al de una lista de direccionamientos.

Non-native CP name(s) (Nombre o nombres de CP no nativos) constituye la siguiente solicitud. Este parámetro se usa para especificar la red o redes no nativas a las que se aplica esta tabla de correlaciones de CoS.

Al igual que ocurre con los nombres de LU de una lista de direccionamientos, puede acabar con antelación cualquiera de los nombres de FQCP en cualquier

punto, utilizando un carácter comodín "*" final. Esto le permitirá especificar un rango de nombres de FQCP no nativos en una o varias redes no nativas. No incluya un carácter comodín en medio de un nombre FQCP.

Una tabla de correlaciones de CoS de un nodo de frontera ampliado puede tener una carácter comodín autónomo "*" como uno de los nombres de CP no nativos. Dicha tabla será conocida como la *default CoS mapping table* (tabla de correlaciones de CoS por omisión) y el nodo de frontera ampliado la utilizará siempre que ninguna otra tabla tenga un nombre de CP que coincida con la red no nativa.

CoS name pairs (Pares de nombres de CoS) constituye la parte final de la configuración de una tabla de correlaciones de CoS. En este punto, se le solicitará uno o varios pares de nombres de CoS. Cada nombre de CoS está formado por un nombre de CoS nativo seguido del nombre de CoS correspondiente utilizado en la red no nativa.

Extended Border Node usa esta tabla para hacer una conversión de una red nativa a una red no nativa y viceversa. Si necesita correlacionar varios nombres de CoS nativos en un nombre de CoS no nativo común deberá configurar un par de nombres de CoS por cada correlación posible. Asimismo, puede que necesite correlacionar varios nombres de CoS no nativos en un nombre de CoS nativo común y esta operación puede realizarla configurando un par de nombres de CoS por cada correlación posible. Si en una tabla existen varias correlaciones posibles, Extended Border Node usará la primera correlación exacta que encuentre.

Cada tabla de correlación de CoS puede tener una pareja de nombres de CoS donde el nombre de CoS no nativo sea un carácter comodín "*". Se trata de la entrada de la *default CoS mapping* (correlación de CoS por omisión) para dicha tabla y se utiliza para convertir todos los nombres de CoS no nativos y no reconocidos en un único nombre de CoS nativo. Cada tabla de correlaciones de CoS puede tener una de estas entradas de correlaciones por omisión. No se puede codificar nunca un "*" como nombre de CoS nativo.

Direccionamiento de alto rendimiento

Consulte la Tabla 2 en la página 23 para obtener una lista de los puertos que dan soporte a HPR.

Consulte "Requisitos de configuración de APPN" en la página 25 para obtener información sobre cómo configurar los protocolos que dan soporte al direccionamiento APPN y HPR sobre los DLC directos en el direccionador. En el caso de los parámetros de HPR como el temporizador de conmutación de vías de acceso y el de reintento, la configuración se efectúa en el nivel de nodo y no se especifica en adaptadores individuales.

DLUR

Consulte la Tabla 2 en la página 23 para obtener una lista de los puertos que dan soporte al DLUR.

Configuración de los puntos focales

Los puntos focales pueden ser explícitos o implícitos. Los puntos focales explícitos se configuran en el mismo punto focal. No es necesario configurarlos en el direccionador.

Por otra parte, los puntos focales implícitos se configuran en el direccionador. Se configuran con el mandato **add focal_point**. Añada primero el punto focal implícito primario. Si añade otro punto focal, se conocerá como el primer punto focal implícito de seguridad. Si añade otro más, éste se conocerá como el segundo punto focal implícito de seguridad. Puede añadir hasta ocho puntos focales implícitos de seguridad hasta conseguir un total de 9.

Para suprimir un punto focal use el mandato **delete focal_point**. Se le solicitará el nombre del punto focal que desee suprimir. Cuando suprima el nombre, los puntos focales restantes conservarán su posición en relación con los demás. Los puntos focales posteriores se añadirán al final de la lista.

No se puede insertar un punto focal en medio de la lista. Deberá suprimir los puntos focales de uno en uno y después volver a entrar la lista completa.

Configuración del tamaño de la cola de retención de alertas

Para configurar el tamaño de la cola de retención de alertas, entre el mandato **set management** y responda a la pregunta Held Alert Queue Size (tamaño de la cola de retención de alertas). La cola toma por omisión un tamaño de 10 alertas y los valores válidos están en el rango incluido entre 0 y 255 alertas.

A medida que aumente el tamaño de la cola de retención de alertas, necesitará memoria adicional. Si la establece en un valor elevado, es posible que desee ajustar el valor Maximum Shared Memory (Memoria compartida máxima). Consulte "Ajuste del nodo APPN" en la página 40 para obtener información adicional.

Definición de las características de los grupos de transmisión (TG)

Cuando configura APPN en el direccionador, puede especificar las características del grupo de transmisión (TG) para la estación de enlace que define una conexión entre el nodo de red del direccionador y un nodo adyacente. Estas características como, por ejemplo, la seguridad de un enlace o su capacidad efectiva, las usa APPN al calcular una ruta óptima o de menos peso entre nodos de la red APPN.

APPN, en el direccionador, usa un conjunto de características de TG por omisión por cada puerto (o puerto DLSw). Estos valores por omisión, definidos por el parámetro *default TG characteristics* (Características de TG por omisión) se aplican a todos los TG para estaciones de enlace definidas en un puerto, a menos que el parámetro *modify TG characteristics* (Modificar características de TG) altere temporalmente las características para una estación de enlace concreta.

Estas características de TG por omisión también se usan para estaciones de enlace dinámicas establecidas cuando un nodo adyacente solicita una conexión con el nodo de red del direccionador, pero no tiene una definición de estación de enlace definida previamente en dicho nodo. El parámetro *Service any node* (servir a cualquier nodo) deberá estar habilitado.

Puede cambiar los parámetros siguientes usando la interfaz **talk 6>** del direccionador, así como el Configuration Program:

- time cost (coste en tiempo)
- byte cost (coste en bytes)
- user-defined TG characteristics 1 - 3 (Características 1 - 3 del TG definidas por el usuario)
- effective capacity (capacidad efectiva)
- propagation delay (retardo de propagación)
- security (seguridad)

Calculo de rutas de APPN usando las características de los TG

La función de cálculo de rutas de APPN usa una definición de CoS para los TG que es una tabla que contiene filas de rangos de características de TG. Cada fila define un rango determinado para cada una de las ocho características de los TG y el peso del TG correspondiente para dicha fila. APPN empieza al principio de la tabla y continúa hacia abajo hasta que los ocho valores del parámetro de las características del TG entren dentro de los rangos dados para dicha fila. A continuación, APPN asigna el peso de dicha fila como peso de TG para el enlace. También hay una definición de CoS para nodos que calcula el peso de un nodo. La función de cálculo de la ruta continúa hasta encontrar el recorrido con el menor peso combinado de TG y nodos. Esta es la ruta de menos peso.

Veamos un ejemplo de cómo las características del TG se usan para influir en la selección de una ruta a través de un nodo de red APPN. Supongamos que una ruta que va del direccionador de nodo de red A al direccionador de nodo de red D puede pasar a través del direccionador de nodo de red B o el C. En este ejemplo, el direccionador A define las conexiones del puerto serie PPP al direccionador B y el C. No obstante, la conexión del direccionador A al direccionador B tiene un enlace de 64 kbps, mientras que la conexión de A a C tiene un enlace de menor velocidad de 19,2 kbps.

Para asegurarse de que se considere más deseable la conexión de mayor velocidad que va del direccionador A al direccionador B para direccionar tráfico interactivo APPN, se modificará la característica de capacidad efectiva de TG para la estación de enlace asociada a este recorrido. Supongamos que en este caso, el valor por omisión para la capacidad efectiva es X'38', el cual representa correctamente una velocidad de enlace de aproximadamente 19,2 kbps. No obstante, la capacidad efectiva se cambiará a X'45' para representar adecuadamente el enlace de 64 kbps. Dado que la capacidad efectiva del TG del direccionador A al direccionador B es ahora de X'45', se asignará menos peso a este recorrido en el archivo de CoS para el tráfico interactivo. Por consiguiente, se representará la conexión del direccionador A al B, como más deseable que la conexión del direccionador A al C.

También puede cambiar las características de TG si desea favorecer, voluntariamente, algunos TG para selección de ruta. Además de las cinco características de TG arquitecturadas, existen otras tres características de TG definidas por el usuario. Puede definir estas características para inclinar el cálculo de la selección de ruta a favor de algunos recorridos.

Nota: Para los puertos DLSw, las características de TG que defina afectarán únicamente a la selección de rutas entre nodos APPN sobre estos puertos DLSw. Estas características no tendrán ningún efecto directo sobre el direccionamiento intermedio efectuado por DLSw en nombre de APPN.

Opciones de CoS

Puede usar una plantilla para crear nuevos nombres de CoS definidos por el usuario y definiciones asociadas para TG y nodos que pueden usarse con nombres de modalidades nuevas o correlacionados con nombres de modalidades ya existentes.

Además, puede crear nombres de modalidades nuevas que pueden correlacionarse con nombres de CoS existentes.

Cada archivo de definiciones de CoS se identifica mediante un nombre de CoS y contiene una prioridad de transmisión asociada y una tabla de rangos de características de nodo y de TG aceptables que APPN compara con características de nodo y de TG reales para determinar pesos para TG y nodos a partir de los cuales APPN calculará la ruta de menos peso para la sesión. Con el Configuration Program puede:

- Ver un archivo de definiciones de CoS:
 - Ver la prioridad de transmisión
 - Ver una lista de referencias de filas de nodos junto con sus pesos correspondientes
 - Ver una lista de referencias de filas de TG junto con sus pesos correspondientes
- Seleccionar tablas de COS ATM o estándar como plantillas para definir un archivo de definiciones nuevo de CoS definidos por el usuario con un nombre de CoS nuevo:
 - Importar un archivo de CoS definido por IBM para usar como plantilla
 - Importar un archivo de definiciones de CoS definido por el usuario, exportado previamente para usar como plantilla
- Definir los rangos máximo y mínimo de las características de TG definidas por el usuario dentro de una definición de CoS definida por IBM.

Nota: En una definición de CoS definida por IBM, puede editar únicamente los rangos de las características de TG definidas por el usuario.

Usando el Configuration Program o **talk 6** puede:

- Utilizar las tablas de CoS estándar o las tablas de CoS mejoradas (para ATM).
- Definir un nombre de modalidad nuevo y su correlación con un nombre de CoS.
- Cambiar una correlación entre un nombre de modalidad y un nombre de CoS:
 - Volver a correlacionar un nombre de modalidad definido por IBM con un nombre de CoS distinto.
 - Volver a correlacionar un nombre de modalidad definido por el usuario especificado previamente, con un nombre de CoS distinto.

Consulte el análisis detallado acerca de los servicios de direccionamiento y topología en el manual *IBM SNA APPN Architecture Reference* si desea obtener una descripción de las tablas de CoS estándar y ATM.

Ajuste del nodo APPN

El rendimiento del nodo de red APPN del direccionador puede ajustarse de dos formas:

- Mediante la selección manual de los valores de los parámetros de ajuste *maximum shared memory* (memoria compartida máxima), *percent of APPN shared memory to be used for buffers* (porcentaje de memoria compartida APPN que se utilizará para los almacenamientos intermedios) y *maximum cached directory entries* (número máximo de entradas de directorio en antememoria) utilizando la opción Programa de configuración o **talk 6** de la interfaz de línea de mandatos.

Consulte las páginas de soporte del direccionador de Web y obtendrá una herramienta que podrá utilizar para calcular la memoria necesaria para APPN y otros componentes de direccionador.

- Seleccionando valores para los parámetros *maximum number of ISR sessions* (número máximo de sesiones de ISR), *maximum number of adjacent nodes* (número máximo de nodos adyacentes) y otros parámetros que aparecen en la Tabla 9 en la página 131 y haciendo que el algoritmo de ajuste calcule automáticamente los valores de los parámetros *maximum shared memory* y *maximum cached directory entries*.

Use el Programa de configuración para invocar el algoritmo de ajuste.

El parámetro *maximum shared memory* influye en la cantidad de almacenamiento disponible para el nodo de red APPN para efectuar operaciones de red. Puede permitir que el direccionador escoja un valor por omisión para este valor que sea válido en general en base a la memoria instalada.

El parámetro *maximum cached directory entries* influye en la cantidad de información de directorio que se almacenará o se pondrá en antememoria para reducir el tiempo necesario para localizar un recurso de la red.

Por lo general, ajustar el nodo de red APPN implica un compromiso entre el rendimiento del nodo y el uso del almacenamiento. Cuanto mejor sea el rendimiento, más almacenamiento será necesario.

Notas de ajuste

1. Los valores del parámetro de ajuste deben reflejar el crecimiento anticipado de la red.
2. Si define redes de conexiones dentro de la red APPN y prevé que la mayoría de los nodos finales iniciarán sesiones de LU-LU con otros nodos finales en la misma red de conexiones, deberá establecer el parámetro *maximum number ISR sessions* en un valor más pequeño (1). Si usa las redes de conexiones de esta manera, reducirá los requisitos de memoria compartida para el nodo de red del direccionador ya que la mayoría de las sesiones de LU-LU no pasarán por el componente APPN del direccionador.
3. Dado que el parámetro *maximum shared memory* influye en la asignación de almacenamiento dentro del direccionador, deberá proceder con cuidado cuando defina explícitamente este parámetro. Utilice el valor por omisión configurado automáticamente a menos que efectúe un análisis más detallado mediante la herramienta de almacenamiento del direccionador.

Servicio de nodo (Rastreo)

La opción APPN Node Service (Traces) (Servicio de nodo APPN - rastreo) le permite empezar cualquier rastreo de APPN a través de **talk 6** o el Configuration Program. Los rastreos se activan cuando el archivo de configuración se aplica al direccionador y seguirán así hasta detenerse cuando se aplique una configuración nueva que los detenga.

Nota: La ejecución de rastreos en el direccionador puede influir en su rendimiento. Sólo deben iniciarse los rastreos cuando sea necesario para el servicio del nodo y deberán detenerse tan pronto como se reúna la cantidad de información necesaria.

Los rastreos APPN se agrupan en las 5 categorías siguientes:

- Los rastreos de nivel de nodo especifican rastreos que afectan globalmente al nodo de red APPN.
- Los rastreos de señales interproceso especifican rastreos de nivel de componentes sobre las señales entre los componentes de APPN.
- Los rastreos de entrada y salida de módulos especifican los rastreos de nivel de componente sobre la entrada y salida de los módulos APPN.
- Los rastreos generales especifican rastreos de nivel de componente sobre los componentes APPN.
- Los rastreos varios especifican información de rastreo sobre transmisiones y recepciones de DLC.

Ahora puede habilitar/inhabilitar todos los distintivos de rastreo a través de Talk 6 utilizando la pregunta Turn all trace flags off (Desactivar todos los distintivos de rastreo) realizada con el mandato **set trace** o utilizando el Configuration Program. Consulte la página 136 si desea obtener más información.

Ahora puede filtrar los datos de rastreo de transmisiones y recepciones de control de enlace de datos según el tipo de mensaje o especificando la longitud máxima de los datos por paquete a rastrear. Consulte la Tabla 15 en la página 150 para obtener más información.

Estadísticas de nodo y de contabilidad

Las sesiones intermedias son sesiones de LU-LU que pasan a través del nodo de red APPN, pero cuyos puntos finales (origen y destino) radican fuera del nodo de red. La información acerca de las sesiones intermedias se genera a través del componente ISR del nodo de red y entra dentro de una de las dos categorías siguientes:

- Nombres de sesiones intermedias y contadores
- Datos del vector de control de selección de ruta (RSCV) para las sesiones intermedias

Si habilita el parámetro Collect intermediate session information (Recoger información de sesión intermedia), instruirá al direccionador para que tome los nombres de sesión y lea los contadores de todas las sesiones intermedias activas. Si habilita el parámetro Save RSCV information for intermediate sessions (Guardar información de RSCV para sesiones intermedias) instruirá al direccionador para que recoja datos de RSCV para sesiones intermedias activas. Estos datos RSCV son útiles para supervisar rutas de sesión. En ambos casos, puede recuperar los datos

en sesiones activas emitiendo los mandatos de SNMP **get** y **get-next** para variables de la APPN Management Information Base (Base de información de gestión de APPN - MIB).

Por omisión, la función Collect intermediate session information está inhabilitada. Puede habilitarla utilizando el Configuration Program o el mandato **set management** de Talk 6. Una vez habilitada, podrá controlarla, incluyendo la inhabilitación y habilitación, usando los mandatos **set** de SNMP para la MIB de contabilidad de APPN.

Nota: Esta función usa una cantidad significativa de memoria APPN. Debe configurar APPN con la memoria necesaria antes de habilitar la recogida de información ISR.

Por motivos de contabilidad, puede mantener registros de las sesiones intermedias que pasen por el nodo de red. Los registros de datos se pueden crear y almacenar en la memoria del direccionador. Debe usarse SNMP para recuperar datos de registros de contaje almacenados en la memoria local del direccionador.

Notas:

1. Puede habilitar la recogida de datos de sesiones intermedias activas (contadores de sesiones y características de sesión) en las variables SNMP MIB explícita o implícitamente.

Para habilitar la recogida explícitamente, establezca el parámetro Collect intermediate session information en yes (sí).

Para habilitar implícitamente la recogida, establezca Create intermediate session records (Crear registros de sesiones intermedias) en yes. Este valor alterará temporalmente el de Collect intermediate session information.

2. Los cambios de configuración en los parámetros de contabilidad de APPN efectuados usando la interfaz Talk 6 no entrarán en vigor hasta que el direccionador o la función APPN del direccionador se reinicien. No obstante, puede realizar los cambios interactivamente, emitiendo los mandatos **set** de SNMP para modificar las variables APPN MIB asociadas a los parámetros de configuración. Consulte el manual *Guía del usuario de software* para obtener una lista de estas variables de MIB.
3. Los datos sobre RSCV de sesiones intermedias se obtienen examinando la solicitud BIND usada para activar una sesión entre dos LU. Los datos de RSCV no se recogen para sesiones que ya se hayan establecido ya que la información de BIND para dichas sesiones no está disponible.
4. Los datos de las sesiones intermedias no se recogen para sesiones de HPR ya que dichas sesiones no forman parte de HPR. Si el direccionador contiene una frontera ISR/HPR, los datos de la sesión intermedia se recogerán cuando pasen por dicha frontera.

Algoritmo de reintento del DLUR

Si se interrumpe la comunicación entre el DLUR y el DLUS, se usará el algoritmo siguiente para restablecerla:

Si Perform retries to restore disrupted pipe (Efectuar reintentos para restaurar el conducto interrumpido) es No:

- Si el DLUR recibe un UNBIND de no interrupción (código de detección X'08A0 000A'), esperará indefinidamente a que un DLUS vuelva a establecer el conducto interrumpido.
- Si el conducto falla por cualquier otra razón que no sea un UNBIND de no interrupción, el DLUR intentará alcanzar el DLUS primario una vez. Si no lo consigue, el DLUR intentará alcanzar el DLUS de seguridad. Si el DLUR no puede alcanzar el DLUS de seguridad, esperará indefinidamente a que un DLUS restablezca el conducto interrumpido.

Si Perform retries to restore disrupted pipe está en Yes (sí), el DLUR intentará volver a establecer el conducto basándose en los siguientes parámetros de configuración:

- Delay before initiating retries (Retardo antes de iniciar los reintentos)
- Perform short retries to restore disrupted pipe (Efectuar reintentos cortos para restaurar el conducto interrumpido)
- Short retry timer (Temporizador de reintento corto)
- Short retry count (Contador de reintento corto)
- Perform long retries to restore disrupted pipe (Efectuar reintentos largos para restaurar el conducto interrumpido)
- Long retry timer (Temporizador de reintento largo)

Hay dos casos que determinan el algoritmo de reintento:

- En caso de recibir un UNBIND de no interrupción:
 1. Espera el tiempo especificado por el parámetro Delay before initiating retries. Este retardo da tiempo a que entre en función SSCP, en cuyo caso el DLUS nuevo volverá a establecer el conducto sin que el DLUR lleve a cabo ninguna acción.
 2. Intenta acceder al DLUS primario.
 3. Si no lo consigue, intenta acceder al DLUS de seguridad.
 4. Si el intento de acceder al DLUS de seguridad no es satisfactorio, el DLUR realizará otro intento, tal como se describe en los pasos 5 - 7, mientras la DSPU solicita una ACTPU.
 5. Espera el tiempo especificado en el parámetro Long retry timer.

Nota: Si Perform long retries to restore disrupted pipe es No, no se efectuará ningún reintento.
 6. Intenta acceder al DLUS primario.
 7. Si el intento no es satisfactorio, intenta acceder al DLUS de seguridad.

Ejemplo:

- Supongamos los valores de parámetro siguientes:
 - Delay before initiating retries = 120 sec
 - Perform short retries to restore disrupted pipe = yes
 - Short retry timer = 60 sec
 - Short retry count = 2
 - Perform long retries to restore disrupted pipe = yes
 - Long retry timer = 300 sec
- Se produce un fallo en la activación del conducto.
- Espera 120 segundos (el valor de Delay before initiating retries).

- Vuelve a intentar el DLUS primario y, si falla, reintenta el DLUS de seguridad.
 - Si el reintento falla, espera 300 segundos (el valor de Long retry timer), reintenta el DLUS primario y, si falla este reintento, vuelve a intentar el DLUS de seguridad.
 - Si falla el reintento, sigue reintentando el DLUS primario y de seguridad, esperando 300 segundos entre las secuencias de reintento, mientras la DSPU solicita la ACTPU.
- En el resto de los casos de fallo de conducto, el DLUR reintentará el DLUS primario y el DLUS de seguridad inmediatamente después. Si falla, el DLUR:
 1. Esperará el tiempo especificado por el mínimo de los parámetros Short retry timer y Delay before initiating retries.
 2. Intentará acceder al DLUS de reserva.
 3. Si el intento no es satisfactorio, intentará acceder al DLUS de seguridad.
 4. Si la activación del conducto sigue presentando anomalías, el DLUR efectuará tantos reintentos como se especifique en Short retry count (el proceso de reintento se describe en los pasos del 1 al 3).

Si Short retry count se agota, el DLUR realizará reintentos, tal como se define en los pasos del 5 al 7, mientras la DSPU solicite la ACTPU.
 5. Esperará el tiempo especificado en el parámetro Long retry timer.

Nota: Si Perform long retries to restore disrupted pipe es No, no se efectuará ningún reintento.
 6. Intentará acceder al DLUS de reserva.
 7. Si el intento no es satisfactorio, intentará acceder al DLUS de seguridad.

Ejemplo:

- Supongamos los valores de parámetro siguientes:
 - Delay before initiating retries = 120 sec
 - Perform short retries to restore disrupted pipe = yes
 - Short retry timer = 60 sec
 - Short retry count = 2
 - Perform long retries to restore disrupted pipe = yes
 - Long retry timer = 300 sec
- Se produce un fallo en la activación del conducto.
- Reintenta inmediatamente el DLUS primario y de seguridad.
- Si este reintento no es satisfactorio, espera durante 60 segundos (el valor de Short retry timer).
- Reintenta el DLUS primario. Si el reintento falla, reintenta el DLUS de seguridad. Se trata del intento núm. 1 de Short retry count.
- Si es anómalo, espera durante 60 segundos (el valor de Short retry timer).
- Vuelve a intentar el DLUS primario y, a continuación, el DLUS de seguridad. Se trata del intento núm. 2 de Short retry count. Ahora Short retry count estará agotado.

- Si el reintento sigue fallando, espera 300 segundos (el valor de Long retry timer). A continuación, vuelve a intentar el DLUS primario. Si el reintento falla, reintenta el DLUS primario.
- Mientras el reintento falla, sigue reintentando el DLUS primario y el de seguridad, esperando 300 segundos entre las secuencias de reintento, mientras la DSPU solicite la ACTPU.

Implementación de APPN en el direccionador usando DLSw

El direccionador también da soporte a APPN sobre DLSw en cuestiones de conectividad con nodos a través de un asociado DLSw remoto. En la Figura 2 podemos ver un ejemplo. Este soporte permite que los clientes que tengan redes DLSw alcancen APPN sin necesitar un direccionador DLSw externo. También permite que los servidores TN3270 remotos lleguen al sistema principal mediante enlaces DLSw de subárea.

Nota: Se recomienda usar APPN sobre DLC directos cuando estén disponibles, en vez de APPN sobre DLSw. Sin embargo, DLSw local es la única forma que un servidor de TN3270 remoto tiene para poder utilizar enlaces de subárea QLLC X.25 o SDLC para llegar al sistema principal.

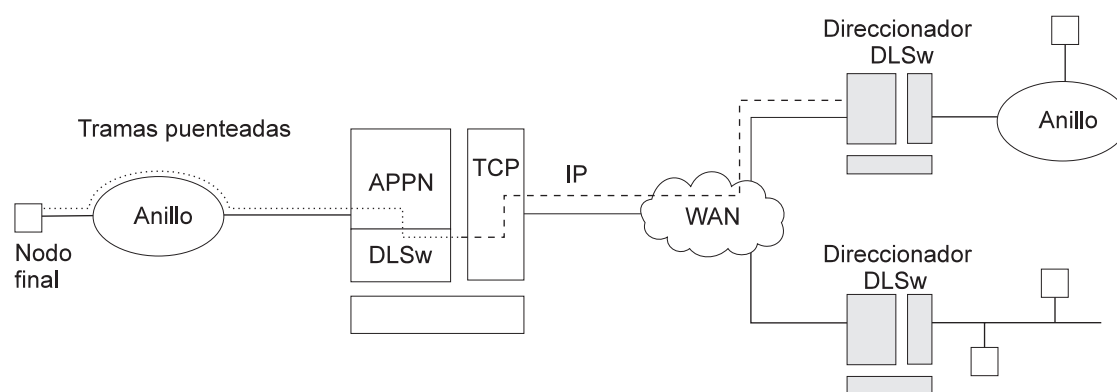


Figura 2. Flujo de datos en una configuración de APPN cuando se usa un puerto DLSw

Restricciones de la configuración de APPN cuando se usa DLSw:

- Sólo un puerto lógico DLSw por cada direccionador
- Uso de una dirección del MAC administrada localmente
- HPR no tiene soporte en los puertos de DLSw
- Los puertos de DLSw no pueden ser miembros de redes de conexiones
- Los TG paralelos no tienen soporte en los puertos de DLSw

Consulte “Configuración del direccionador como nodo de red de APPN” en la página 25 para obtener información sobre cómo configurar APPN usando DLSw.

Cómo usa APPN los puertos DLSw para transportar datos

Cuando se configura APPN en el direccionador para que utilice el puerto de Data Link Switching (Conmutación de enlace de datos - DLSw), DLSw proporcionará una interfaz orientada a conexión (802.2 LLC tipo 2) entre el componente APPN del direccionador y los nodos APPN y SNA conectados a un asociado de DLSw remoto.

Cuando configure un puerto DLSw para APPN en el direccionador, asignará el nodo de red a una dirección MAC exclusiva y una o más direcciones SAP que le

permitirán comunicar con DLSw. La dirección del MAC para el nodo de red está administrada localmente y no debe corresponder a ninguna dirección del MAC física de la red DLSw. Son necesarias varias direcciones SAP sólo cuando esté configurando el servidor de TN3270 para que llegue al sistema principal mediante DLSw y sea necesaria más de una PU dependiente.

Implementación de la red de conexiones APPN Frame Relay BAN

La implementación de una red de conexiones APPN Frame Relay BAN permite definir un puerto APPN Frame Relay que da soporte al formato Frame Relay puentado (BAN) con una red de conexiones.

Un recurso de transporte de acceso compartido (SATF) es un recurso de transmisión, como por ejemplo una red en anillo o Ethernet, donde los nodos conectados al SATF pueden conseguir una conectividad de cualquiera con cualquiera. Esta conectividad permite establecer conexiones directas entre dos nodos, con lo que se elimina el direccionamiento a través de nodos de red intermedios y que los datos correspondientes atravesen varias veces el SATF. No obstante, para conseguir esta conectividad directa, los TG deben estar definidos en cada nodo para el resto de los nodos.

El SATF que aparece en la Figura 3 muestra que el APPN NN del direccionador debe definir una estación de enlace para cada nodo de la red en anillo para iniciar una conexión con cada nodo de ésta. El APPN NN debe saber la dirección DLCI para el enlace Frame Relay y la dirección del MAC de cada nodo de la red en anillo. Si los nodos de la red en anillo desean iniciar una conexión con el APPN NN, deberán definir una estación de enlace en el APPN NN del dispositivo y especificar:

- La dirección BAN DLCI MAC si el dispositivo que conecta la red en anillo a la red frame relay está llevando a cabo la función BAN
- La dirección Boundary Node Identifier MAC si el dispositivo que conecta la red en anillo a la red Frame Relay es un puente

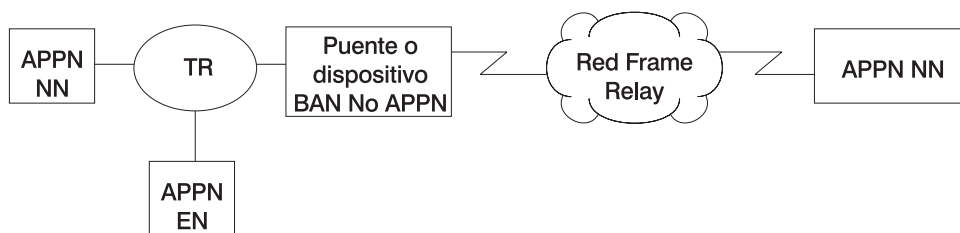


Figura 3. Vista lógica con soporte de red de conexiones BAN/Trama puentada Frame Relay

Nota: En el presente diagrama y en el resto de los diagramas Frame Relay BAN, el APPN reside en el 2210.

La definición de conexiones entre todos los pares de nodos posibles conectados al SATF da como resultado un gran número de definiciones así como un gran número de flujos de actualizaciones de la base de datos de topología circulando por la red. APPN permite que los nodos se conviertan en miembros de una red de conexiones para representar su conexión con el SATF.

La Figura 4 en la página 47 muestra todos los nodos como miembros de la misma red de conexiones. Los nodos usan la red de conexiones para establecer comunicación con el resto de los nodos, por lo que se elimina la necesidad de crear conexiones con el resto de los nodos en el SATF. Para convertirse en miembro de una red de conexiones, debe "conectarse" el puerto de un nodo APPN a dicha red definiendo una interfaz de red de conexiones. Cuando el puerto se activa, el componente APPN crea un TG de red de conexiones con un nodo de direccionamiento virtual (VRN). Este TG identifica la conexión directa desde el puerto con la red de conexiones. El nombre del CP del VRN es el de la red de conexiones.

Dado que la conectividad está representada por un TG de un nodo determinado con un VRN, el servidor de nodos de red puede usar los servicios de direccionamiento y topología normales (TRS) para establecer la vía de acceso directa entre cualquier par de nodos conectados a la red de conexiones. La información de señalización DLC se devuelve desde el nodo de destino durante el proceso de localización normal para habilitar al nodo de origen para que establezca directamente una conexión con el nodo de destino.

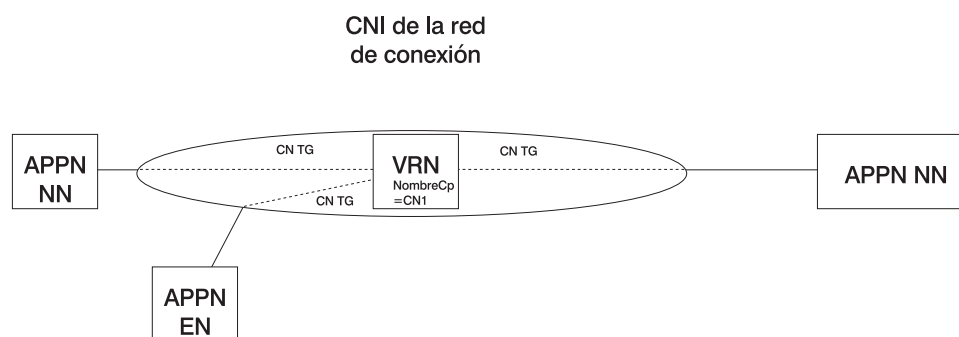


Figura 4. Trama puenteada de APPN Frame Relay con la red de conexiones BAN

El uso de las redes de conexiones APPN Frame Relay BAN tiene las limitaciones siguientes:

- La misma red de conexiones puede definirse en un único SATF.
- Todos los puertos de Frame Relay que pertenezcan a la misma red de conexiones del direccionador deben usar el mismo número DLCI para conectarse con la red Frame Relay.
- Cuando se usa el puenteo en vez de BAN, todos los puertos de Frame Relay que pertenezcan a la misma red de conexiones del direccionador deben tener el mismo par de direcciones BNI MAC/SAP definido.
- No pueden establecerse sesiones de CP-CP sobre enlaces establecidos a través de una red de conexiones.

Ejemplos de definiciones de red de conexiones APPN Frame Relay BAN

Ejemplo 1

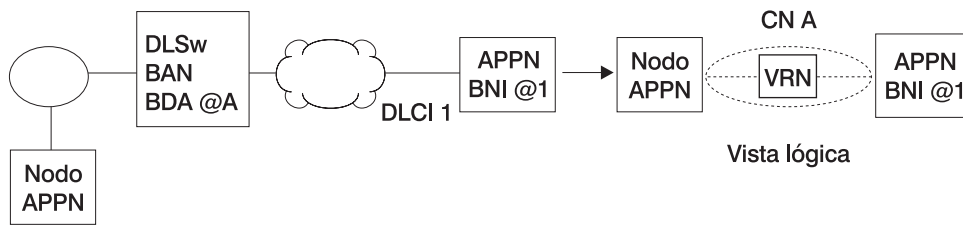


Figura 5. Red de conexiones única que usa BAN con 1 puerto de Frame Relay

Nota: Debe definirse la dirección BDA en la definición de red de conexiones.

Ejemplo 2

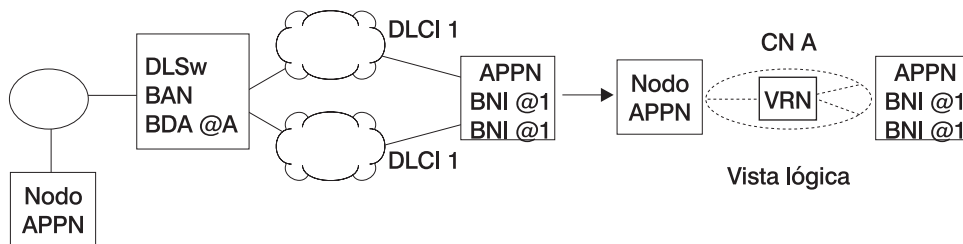


Figura 6. Red de conexiones única que usa BAN con varios puertos Frame Relay

Notas:

1. Debe especificarse el mismo número DLCI en ambos puertos.
2. Debe definirse la dirección BDA en la definición de red de conexiones.
3. Las direcciones de BNI de ambos puertos pueden ser las mismas o diferentes.
4. Si el nodo APPN inicia la conexión con el dispositivo, el puerto APPN que se elige para la conexión dependerá de qué puerto responde primero a la trama de prueba.

Ejemplo 3

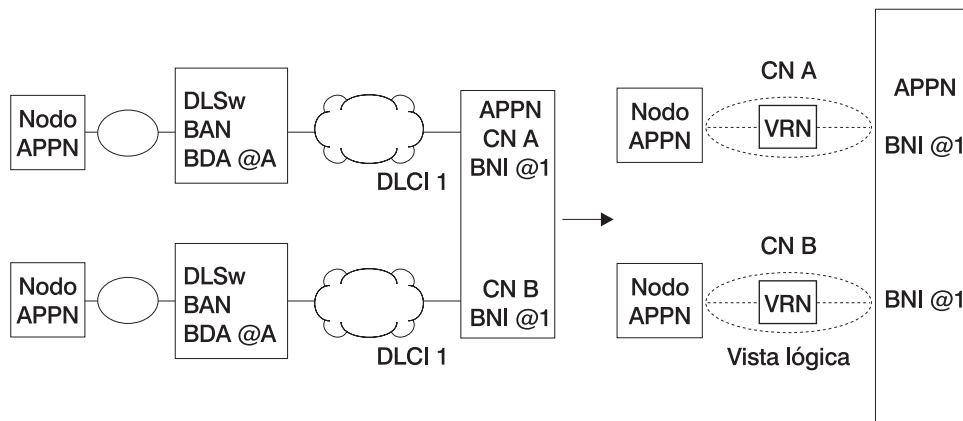


Figura 7. Diversas redes de conexiones que usan BAN

Notas:

1. Esta configuración requiere dos definiciones de red de conexiones ya que hay dos SATF.
2. El número DLCI especificado en los puertos puede ser el mismo o diferente.
3. Debe definirse la dirección BDA MAC en la definición de la red de conexiones.
4. La dirección BNI MAC especificada en los puertos puede ser la misma o diferente.

Ejemplo 4

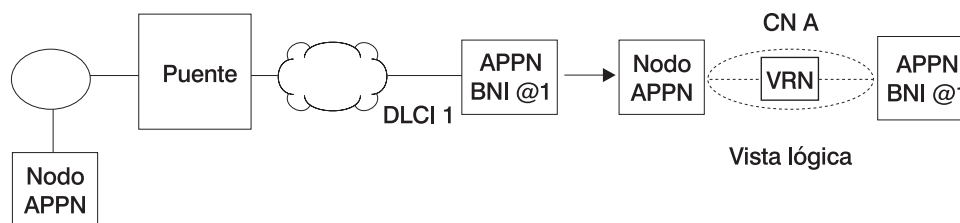


Figura 8. Red de conexiones única que usa el puenteo con 1 puerto de Frame Relay

Notas:

1. La dirección BDA no está definida en la definición de red de conexiones.

Ejemplo 5

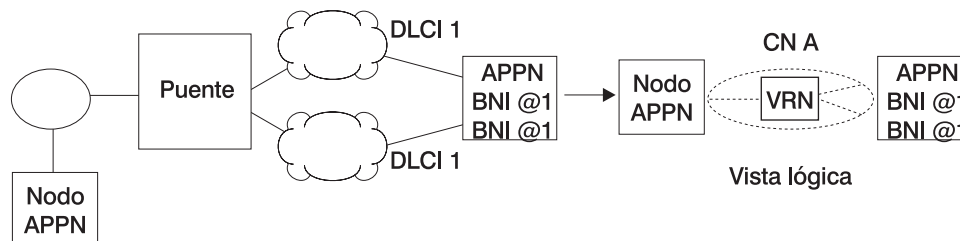


Figura 9. Red de conexiones única que usa el puenteo con diversos puertos Frame Relay

Notas:

1. Debe especificarse el mismo número DLCI en ambos puertos.
2. Debe especificarse el mismo par SAP/dirección BNI MAC en ambos puertos.
3. No se ha especificado la dirección BDA MAC en la definición de la red de conexiones.
4. Si el nodo APPN inicia la conexión con el dispositivo, el puerto APPN que se elige para la conexión dependerá de qué puerto responda primero a la trama de prueba.

Ejemplo 6

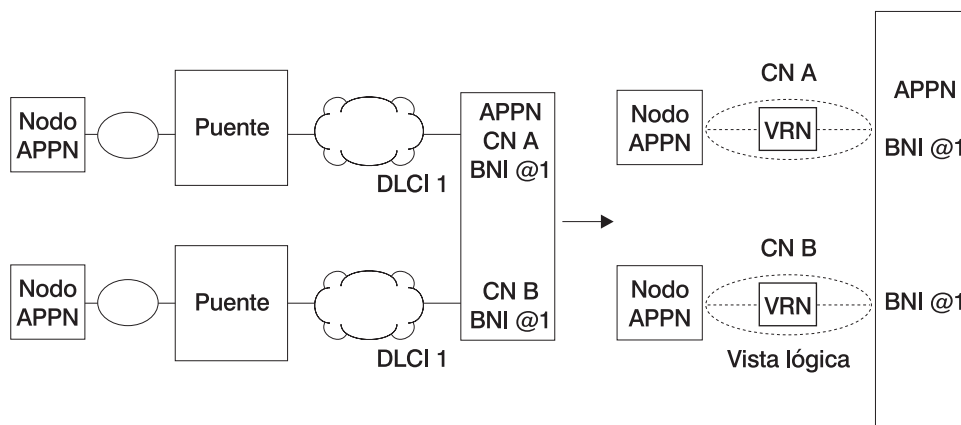


Figura 10. Diversas redes de conexiones que usan el pueneteo

Notas:

1. Esta configuración requiere dos definiciones de red de conexiones ya que hay dos SATF.
2. El número DLCI especificado en los puertos puede ser el mismo o diferente.
3. La dirección BDA MAC no está definida en la definición de la red de conexiones.
4. El par dirección BNI MAC/SAP especificado en los puertos puede ser el mismo o diferente.

Listas de parámetros del nivel de puerto

Use las tablas siguientes para configurar los puertos de APPN:

- Configuración del puerto en la página 155
- Definición de puertos en la página 163
- Características del TG del puerto por omisión en la página 167
- Características LLC del puerto por omisión en la página 172

Listas de parámetros del nivel de enlace

Use las tablas siguientes para configurar las estaciones de enlace de APPN:

- Valores por omisión de HPR en la página 175
- Estaciones de enlace - Detalle en la página 176
- Modificación de las características de los TG en la página 190
- Modificación del servidor de LU dependientes en la página 192
- Modificación de las características del LLC en la página 193
- Modificación de los valores por omisión de HPR en la página 195

Lista de parámetros de LU

Use la tabla siguiente para configurar una LU:

- Nombre de la LU del nodo final LEN en la página 197

Listas de parámetros del nivel de nodo

Use las tablas siguientes para configurar un nodo APPN:

- Características básicas del nodo local en la página 119
- Direccionamiento de alto rendimiento (HRP) en la página 125
- Temporizador de HPR y opciones de reintento en la página 125
- Peticionario de LU dependientes en la página 128
- Red de conexiones - Detalle en la página 198
- Características de los TG (Red de conexiones en la página 203
- APPN COS - Puerto adicional a CN en la página 207
- Rastros de nivel de nodo en la página 136
- Rastros de señales entre procesos en la página 141
- Rastros de la entrada y salida en módulos en la página 144
- Rastros de nivel de componentes generales en la página 146
- Gestión de nodos APPN en la página 152
- "TN3270E" en la página 218
- Tabla 38 en la página 211
- Tabla 39 en la página 215

Notas sobre la configuración de APPN

Los ejemplos siguientes muestran parámetros especiales que hay que tener en cuenta cuando se configuran varias funciones para transportar tráfico de APPN.

Nota: Estos ejemplos muestran ejemplos de impresiones. Es posible que la impresión que obtenga no sea exactamente igual a la que se muestra aquí.

Nota: En algunos ejemplos de configuración, los resultados de un mandato **talk 6 list** pueden mostrar más configuración de la que presentamos en el ejemplo. No obstante, el ejemplo mostrará todo lo que sea único de la configuración.

Configuración de un circuito permanente usando RDSI

Este ejemplo muestra una configuración de un circuito permanente que usa Frame Relay sobre RDSI desde el nodo 21 al nodo 1.

Nota: Un circuito permanente se configura estableciendo el valor del temporizador de desocupación en 0.

```
*****
**** Configuring a PERMANENT circuit via RDSI from NN21 to NN1
**** Using Frame Relay over RDSI
*****
```

```
Config>n 6
Circuit configuration
FR Config>li a11

Base net = 3
Destination name = 2210-01
Circuit priority = 8
Destination address: subaddress = 99195551234:

Inbound destination name = 2210-01
Inbound dst address: subaddress = 99195551000:

Inbound calls = allowed
Idle timer = 0 (fixed circuit) 1
SelfTest Delay Timer = 150 ms
```

FR Config>ex

```
*****
**** Verify that a FR PVC is defined to NN1. This is required for APPN
*****
```

```
Config>n 6
Circuit configuration
FR Config>en
Frame Relay user configuration
FR Config>li perm
```

```
Maximum PVCs allowable = 64
Total PVCs configured = 1
```

Circuit Name	Circuit Number	Circuit Type	CIR in bps	Burst Size	Excess Burst
2210-21-i6	16	Permanent	64000	64000	0

= circuit is required and belongs to a required PVC group

```

FR Config>ex
Config>p appn
APPN user configuration
APPN config>add p
APPN Port
Link Type: (P)PP, (F)RAME RELAY, (E)THERNET, (T)OKEN RING,
(S)DLC, (X)25, (D)LSw, (A)TM, (IP) [ ] ? f
Interface number(Default 0): [0]?6
Port name (Max 8 characters) [FR006 ] ?
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
    Service any node: (Y)es (N)o[Y]?
    Limited resource: (Y)es (N)o[N]?
    High performance routing: (Y)es (N)o [Y]?
Maximum BTU size (768-2044) [2044 ] ?
    Percent of link stations reserved for incoming calls (0-100) [0]?
    Percent of link stations reserved for outgoing calls (0-100) [0 ] ?
    Local SAP address (04-EC) [4]?
    Support bridged formatted frames: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y ] ?
The record has been written.
APPN config>add li
APPN Station
Port name for the link station [ ] ? fr006
Station name (Max 8 characters) [ ] ? tonnliSDN
Station name (Max 8 characters) [ ] ? tonnliS
    Limited resource: (Y)es (N)o[N]?
    Activate link automatically (Y)es (N)o[Y]?
    DLCI number for link (16-1007) [16]?
Adjacent node type: 0 = APPN network node, 1 = APPN end node
2 = LEN end node, 3 = PU 2.0 node [0]?
    High performance routing: (Y)es (N)o [Y]?
Edit Dependent LU Server: (Y)es (N)o [N]?
    Allow CP-CP sessions on this link (Y)es (N)o [Y]?
    CP-CP session level security (Y)es (N)o [N]?
    Configure CP name of adjacent node: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y ] ?
The record has been written.
APPN config>ex

```

```

APPN config>li a11
NODE:
  NETWORK ID: STFNET
  CONTROL POINT NAME: NN21
  XID: 00000
  APPN ENABLED: YES
  MAX SHARED MEMORY: 4096
  MAX CACHED: 4000
DLUR:
  DLUR ENABLED: YES
  PRIMARY DLUS NAME: NETB.MVSC
CONNECTION NETWORK:
  CN NAME          LINK TYPE  PORT INTERFACES
-----
COS:
  COS NAME
  -----
  BATCH
  BATCHSC
  CONNECT
  INTER
  INTERSC
  CPSVCMG
  SNASVCMG
  USRBAT
  USRNOT
MODE:
  MODE NAME  COS NAME
  -----
  #USRBAT   #USRBAT
  #USRNOT   #USRNOT
PORT:
  INTF  PORT  LINK  HPR  SERVICE  PORT
  NUMBER NAME TYPE  ENABLED ANY  ENABLED
-----
0      TR000  IBMTRNET  YES  YES  YES
      1      SDLC001  SDLC  NO   YES  YES
      254    DLS254  DLS   NO   YES  YES
      6      FR006   FR    YES  YES  YES  3
STATION:
  STATION  PORT  DESTINATION  HPR  ALLOW  ADJ  NODE
  NAME     NAME  ADDRESS      ENABLED  CP-CP  TYPE
-----
  TONN25   TR000  0004ACA2A407  YES  YES  0
  TONN31   TR000  4FFF00001031  YES  NO   0
  SDLC1    SDLC001  C1            NO   NO   2
  TONN103  DLS254  400000000103  NO   NO   0
  TONN11S  FR006   16           YES  YES  0  4
LU NAME:
  LU NAME          STATION NAME  CP NAME
-----
APPN config>

```

Nota:

- 1** Idle timer = 0 representa un circuito fijo
- 2** El PVC de Frame Relay está definido
- 3** Este es el puerto de RDSI
- 4** Esta es la estación de enlace

Configuración de APPN sobre circuitos de marcación bajo pedido

APPN tiene soporte en los circuitos de marcación bajo pedido para los tipos de DLC siguientes:

- APPN/PPP/RDSI
- APPN/FR/RDSI
- APPN/PPP/V.25 bis
- APPN/PPP/V.34

Consulte el manual *Guía del usuario de software* para obtener información adicional acerca de los circuitos de marcación bajo pedido.

Consideraciones sobre el nodo PU 2.1

Cuando configure una estación de enlace de APPN para nodos PU 2.1 sobre un enlace de marcación bajo pedido, debe especificar *yes* (sí) en el parámetro de la estación de enlace *limited resource* (recurso limitado). Esto permitirá que APPN:

- Considere este enlace como viable para usarlo para el cálculo de ruta, incluso aunque el enlace no esté en realidad activo. El enlace se activará automáticamente durante la activación de una sesión de LU-LU para una sesión que necesite usarla.
- Desactive la estación de enlace cuando ninguna sesión activa use este enlace.

No debe configurar sesiones de CP-CP sobre un enlace de marcación bajo pedido. Se trata de sesiones persistentes. Es decir, son sesiones que deben permanecer activas mientras el enlace también lo esté. Dado que en este caso la cuenta de sesión activa no se pondrá en cero, el enlace permanecerá activo.

Nota: Si especifica *yes* en el parámetro *limited resource* para un nodo PU 2.1, deberá especificar también un CPNAME adyacente y un número de TG dentro del rango incluido entre 1 y 20.

Consideraciones sobre el nodo PU 2.0

Cuando se configura una estación de enlace de APPN para nodos PU 2.0 sobre un enlace de marcación bajo pedido, puede especificar *yes* en el parámetro de la estación de enlace *limited resource*. Esto permitirá que APPN desactive la estación de enlace cuando ninguna sesión activa la use.

Nota: Si *limited resource* es *yes*, la DSPU (la PU 2.0) o VTAM deberán iniciar la activación del enlace para esta estación de enlace.

Consideraciones sobre el uso del DLUR para dispositivos T2.0 o T2.1

Para los nodos T2.0 o T2.1 que utilicen el DLUR para tráfico de sesiones dependientes, deberán estar activas una sesión de SSCP-PU y una de SSCP-LU para establecer una sesión de LU-LU. Estas sesiones están incluidas en la cuenta de sesiones para el enlace con la DSPU. Por consiguiente, si *limited resource* es *yes*, el enlace permanecerá activo mientras la sesión de SSCP-PU esté activa o las sesiones de LU-LU estén activas sobre este enlace.

Si especifica *no* en el parámetro *limited resource*, la desactivación de enlace estará controlada por el nodo que inició la sesión.

Si activó el enlace con la DSPU debido a una llamada de ésta al nodo del DLUR o una llamada del mencionado nodo a la DSPU (por ejemplo, la estación de enlace con la DSPU está configurada en el direccionador y *activate link automatically* (activar enlace automáticamente) es *yes*, cuando la cuenta de la sesión activa se ponga en cero, APPN DLUR desactivará el enlace si la DSPU solicitó la DACTPU. En dicho caso, si el DLUS envía una solicitud de DACTPU al DLUR, éste desactivará la sesión de SSCP-PU. No obstante, no desactivará el enlace con la DSPU. El DLUR intentará volver a establecer la sesión de SSCP-PU con el DLUS o el DLUS de seguridad hasta que obtenga un resultado satisfactorio o hasta que la DSPU ya no necesite esta sesión.

Si el DLUS activó el enlace con la DSPU y la cuenta de sesión pasa a cero, el APPN DLUR desactivará el enlace únicamente si el DLUS envía una solicitud de DACTPU al DLUR.

A continuación, se muestra un ejemplo de configuración de la marcación bajo pedido. Esta configuración es similar a la conexión permanente RDSI salvo que:

- Debe especificar que el enlace es un recurso limitado.
- Debe definir el nombre del CP adyacente.
- Debe especificar un número de TG.

Los dos extremos del enlace de comunicación se configuran de la misma manera.

Nota: Si permite sesiones de CP-CP en este enlace, éste no se desconectará.

```
*t 6
Gateway user configuration
Config>
*****
**** This is the NN6 configuration for a NN6---NN15 dial on demand link.
**** The NN15 config will look just like this.
**** interface 9 is a Dial On Demand link with destination = NN15
*****
Config>n 9
Circuit configuration
FR Config>li all

Base net                = 6
Destination name        = 2210-15
Circuit priority        = 8

Inbound destination name = 2210-15

Inbound calls           = allowed
Idle timer               = 60 sec 1
SelfTest Delay Timer    = 150 ms

FR Config>ex

*****
**** Configure APPN Port for the Interface
*****

Config>p appn
APPN user configuration
APPN config>add p
APPN Port
Link Type: (P)PP, (F)RAME RELAY, (E)THERNET, (T)OKEN RING,
(S)DLC, (X)25, (D)LSw, (A)TM, (IP) [ ] ? p
Interface number(Default 0): [0 ] ? 9
Port name (Max 8 characters) [PPP009 ] ?
```



```

Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
  Service any node: (Y)es (N)o[Y]?
  Limited resource: (Y)es (N)o [Y ] ? 2
  **** note that limited resource = YES
  High performance routing: (Y)es (N)o [Y]?
  Maximum BTU size (768-2044) [2044 ] ?
  Local SAP address (04-EC) [4]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y ] ?
The record has been written.

*****
**** Configure the linkstation for the DOD link to NN15
*****
APPN config>add 1i
APPN Station
Port name for the link station [ ] ? ppp009
Station name (Max 8 characters) [ ] ? to15dod
  Limited resource: (Y)es (N)o [Y ] ? 2
  **** < note limited resource= YES
  TG Number (1-20) [1 ] ? 3
  **** < note TG number is required input for limited resource
  Adjacent node type: 0 = APPN network node, 1 = APPN end node
  2 = LEN end node [0]?
  High performance routing: (Y)es (N)o [Y]?
  Allow CP-CP sessions on this link (Y)es (N)o [Y ] ? N 4
  **** < Be sure to NOT allow CP-CP sessions, or link won't hang up
  Fully-qualified CP name of adjacent node (netID.CPname) [ ] ? stfnet.NN15
  **** < Adjacent node name required for limited resource links 5
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y ] ?
The record has been written.
APPN config>li a11
NODE:
  NETWORK ID: STFNET
  CONTROL POINT NAME: NN6
  XID: 00000
  APPN ENABLED: YES
  MAX SHARED MEMORY: 4096
  MAX CACHED: 4000
DLUR:
  DLUR ENABLED: YES
  PRIMARY DLUS NAME: NETB.MVSC
CONNECTION NETWORK:
  CN NAME          LINK TYPE  PORT INTERFACES
-----
COS:
  COS NAME
  -----
  BATCH
  BATCHSC
  CONNECT
  INTER
  INTERSC
  CPSVCMG
  SNASVCMG
USRBAT
USRNOT

```

```

MODE:
      MODE NAME  COS NAME
-----
      USRBAT    USRBAT
      USRNOT    USRNOT
PORT:
      INTF      PORT      LINK      HPR      SERVICE  PORT
      NUMBER   NAME      TYPE      ENABLED  ANY      ENABLED
-----
      0         TR000    IBMTRNET  YES      YES      YES
      1         PPP001    PPP       YES      YES      YES
      2         SS        SDLC      NO       YES      YES
      3         SDLC      SDLC      NO       YES      NO
      4         PPP       PPP       YES      YES      NO
      5         TR005    IBMTRNET  YES      YES      YES
      254       DLS      DLS       NO       YES      NO
      17        PPP017    PPP       YES      YES      YES
      9         PPP009    PPP       YES      YES      YES  6
STATION:
      STATION   PORT      DESTINATION  HPR  ALLOW  ADJ NODE
      NAME     NAME     ADDRESS      ENABLED  CP-CP  TYPE
-----
      TONN1    TR000    0004AC4E7505  YES  YES    1
      TONN2    TR000    550020004020  YES  YES    1
      TONN9    TR000    0004AC4E951D  YES  YES    1
      TOPC4    TR000    0004AC9416B4  YES  YES    1
      TOVTAM1  TR000    400000003888  YES  YES    1
      TONN35   PPP001    000000000000  YES  YES    0
      T015D0D  PPP009    000000000000  YES  NO     0  7
LU NAME:
      LU NAME      STATION NAME      CP NAME
-----

```

Nota:

- 1** Temporizador de desocupación > 0 significa marcación bajo pedido
- 2** Se trata de un recurso limitado
- 3** Se requiere un número de TG para un recurso limitado
- 4** No permita sesiones de CP-CP en este enlace
- 5** Proporcione un nombre de CP plenamente calificado
- 6** Este es el puerto
- 7** Esta es la estación de enlace

Configuración del redireccionamiento de la WAN

El redireccionamiento de la WAN le permite configurar una ruta alternativa de tal manera que, si falla un enlace primario, el direccionador iniciará automáticamente una conexión nueva con el destino a través de la ruta alternativa.

Puede usar cualquier tipo de enlace como enlace alternativo así como enlace primario. No es necesario conectar el enlace alternativo con el mismo punto final que el enlace primario.

Si usa HPR en el enlace primario y en el alternativo, cuando el enlace primario falle, la función de conmutación de vías de acceso sin interrupciones de HPR redireccionará automáticamente el tráfico al enlace alternativo, sin interrumpir las sesiones de usuario final.

En el presente ejemplo de configuración, el direccionador que ejecuta la función de redireccionamiento de la WAN está configurado con dos definiciones de estación de enlace de APPN; una estación de enlace se define sobre la interfaz primaria y la otra sobre la interfaz alternativa. El direccionador de destino debe tener habilitado APPN en el puerto. Si dicho direccionador tiene definida una estación de enlace, ésta no deberá intentar activar la conexión para evitar tráfico adicional.

En este ejemplo, Frame Relay es la ruta primaria de NN22 a NN6.

```
*****
**** The configuration is NN22---primary FR
****      ---Alternate WRR to NN6
*****
****
**** This is the NN22 configuration
*****
Ifc 0 Token Ring          CSR 6000000, vector 28
Ifc 1 WAN Frame Relay 1   CSR 81620, CSR2 80D00, vector 93
Ifc 2 WAN PPP            CSR 81640, CSR2 80E00, vector 92
Ifc 3 ISDN Basic        CSR      0, vector 0
Ifc 4 PPP Dial Circuit 2   CSR      0, vector 0
      (Disabled)
Ifc 5 PPP Dial Circuit   CSR      0, vector 0
      (Disabled)
Ifc 6 Frame Relay Dial Circuit CSR      0, vector 0
      (Disabled)

*****
* Ifc 4 is the ALTERNATE with Ifc 1 configured as PRIMARY.
* Note that interface 4 should be 'Disabled' here.
* Wan Reroute function will 'Enable' it when the
* Primary fails
*
* NN6 (2210-06) is going the be the destination of the Wan Reroute
*****
Config>n 4
Circuit configuration
FR Config>li

Base net          = 3
Destination name  = 2210-06 3
Circuit priority  = 8
Destination address: subaddress = 99199991201:
```

```

Outbound calls           = allowed
Idle timer               = 0 (fixed circuit)
SelfTest Delay Timer     = 150 ms

```

```

Config>ex
*****
*
*** Configure the Wan Reroute Primary and Alternate circuit
*
*****

```

```

Config>fea wan 4
WAN Restoral user configuration
WRS Config>en wrs
WRS Config>add alt
Alternate interface number [0] ? 4 2
Primary interface number [0] ? 1 1
WRS Config>li all

```

```

WAN Restoral is enabled.
Default Stabilization Time: 0 seconds
Default First Stabilization Time: 0 seconds

```

[No Primary-Secondary pairs defined]

Primary Interface	Alternate Interface	Enabled	Stab	Stab	Start	Stop
1 - WAN Frame Re	4 - PPP Dial Circuit	No	dflt	dflt	Not Set	Not Set

```

*****
*
*** Set Default and first stabilization times
*
*****
*

```

```

WRS Config>set default firs 30
WRS Config>set def stab 10
WRS Config>li all
WAN Restoral is enabled.
Default Stabilization Time: 10 seconds
Default First Stabilization Time: 30 seconds

```

[No Primary-Secondary pairs defined]

Primary Interface	Alternate Interface	Enabled	Stab	Stab	Start	Stop
1 - WAN Frame Re	4 - PPP Dial Circuit	No	dflt	dflt	Not Set	Not Set

```

WRS Config>en alt
Alternate interface number [0] ? 4
WRS Config>ex

```

```

*****
*
*Configure APPN PORTS and LINKSTATIONS for the
*ALTERNATE and PRIMARY interfaces
*****
Config>p appn
APPN user configuration
APPN config>add p 5
APPN Port
Link Type: (P)PP, (F)RAME RELAY, (E)THERNET, (T)OKEN RING,
(S)DLC, (X)25, (D)LSw, (A)TM, (IP) [ ] ? p
Interface number(Default 0): [0] ? 4
Port name (Max 8 characters) [PPP004] ?
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
    Service any node: (Y)es (N)o[Y]?
    Limited resource: (Y)es (N)o[N]?
    High performance routing: (Y)es (N)o [Y]?
    Maximum BTU size (768-2044) [2044] ?
    Local SAP address (04-EC) [4]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y] ?
The record has been written.
APPN config>add li 6
APPN Station
Port name for the link station [ ] ? ppp004
Station name (Max 8 characters) [ ] ? tonN6WRR
    Limited resource: (Y)es (N)o[N]?
    Activate link automatically (Y)es (N)o[Y]?
    Adjacent node type: 0 = APPN network node, 1 = APPN end node
    2 = LEN end node [0]?
        High performance routing: (Y)es (N)o [Y]?
        Allow CP-CP sessions on this link (Y)es (N)o [Y]?
        CP-CP session level security (Y)es (N)o [N]?
        Configure CP name of adjacent node: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y] ?
The record has been written.
APPN config>add li 6
APPN Station
Port name for the link station [ ] ? fr001
Station name (Max 8 characters) [ ] ? tonn1pri
    Activate link automatically (Y)es (N)o[Y]?
    DLCI number for link (16-1007) [16] ? 121
    Adjacent node type: 0 = APPN network node, 1 = APPN end node
    2 = LEN end node [0]?
        High performance routing: (Y)es (N)o [Y]?
        Allow CP-CP sessions on this link (Y)es (N)o [Y]?
        CP-CP session level security (Y)es (N)o [N]?
        Configure CP name of adjacent node: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y] ?
The record has been written.

```

Uso de APPN

```

APPN config>li all
NODE:
  NETWORK ID: STFNET
  CONTROL POINT NAME: NN22
  XID: 00000
  APPN ENABLED: YES
  MAX SHARED MEMORY: 4096
  MAX CACHED: 4000
DLUR:
  DLUR ENABLED: NO
  PRIMARY DLUS NAME:
CONNECTION NETWORK:
  CN NAME          LINK TYPE  PORT INTERFACES
-----
COS:
  COS NAME
-----
  BATCH
  BATCHSC
  CONNECT
  INTER
  INTERSC
  CPSVCMG
  SNASVCMG
  MODE NAME  COS NAME
-----
PORT:
  INTF   PORT   LINK   HPR   SERVICE   PORT
  NUMBER NAME   TYPE   ENABLED ANY   ENABLED
-----
  0      TR000  IBMTRNET  YES   YES   YES
**** < this is the Primary port
  1      FR001  FR        YES   YES   YES 7
**** < this is the alternate port
  4      PPP004  PPP       YES   YES   YES 8
STATION:
  STATION  PORT   DESTINATION  HPR  ALLOW  ADJ NODE
  NAME     NAME   ADDRESS      ENABLED CP-CP  TYPE
-----
  TONN25   FR001   132         YES  YES    0
  TONN31   FR001   141         YES  NO     0
  TONN103  FR001   153         YES  NO     0
**** < this is the alternate to NN6
  TONN6WRR PPP004  000000000000  YES  YES    0 9
**** < this is the Primary to NN1
  TONN1PRI FR001   121         YES  YES    0 10
LU NAME:
  LU NAME          STATION NAME          CP NAME
-----
APPN config>ex

```

```

*****
*****
*****
Config>
*****
**** The configuration is NN22---primary FR
****          ---Alternate WRR to NN6
****
** This is the NN6 configuration which is the destination side for the
* NN22 Wan Reroute
* interface 17 has the ISDN lid for 2210-22 so when NN22 calls into NN6,
* it will map to interface 17
*
*****
11
Config> n 17
Circuit configuration
FR Config>fea li all

Base net                = 6
Destination name        = 2210-22
Circuit priority        = 8

Inbound destination name = 2210-22

Inbound calls           = allowed
Idle timer              = 0 (fixed circuit)
SelfTest Delay Timer    = 150 ms

FR Config>ex
**** on this side, the interface must be ENABLED all the time
Config>ena in 17
Interface enabled successfully

*****
* Define the APPN PORT; NN22 will call into NN6 and dynamically create
* the linkstation when NN22 does a Wan Reroute.
*
*****
Config>p appn
APPN user configuration
APPN config>add p 12
APPN Port
Link Type: (P)PP, (F)RAME RELAY, (E)THERNET, (T)OKEN RING,
(S)DLC, (X)25, (D)LSw, (A)TM, (IP) [ ] ? p
Interface number(Default 0): [0 ] ? 17
Port name (Max 8 characters) [PPP017 ] ?
Enable APPN on this port (Y)es (N)o [Y]?

```

```

Port Definition
  Service any node: (Y)es (N)o[Y]?
  Limited resource: (Y)es (N)o[N]?
  High performance routing: (Y)es (N)o [Y]?
  Maximum BTU size (768-2044) [2044 ] ?
  Local SAP address (04-EC) [4]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y ] ?
The record has been written.
APPN config>1i a1
NODE:
  NETWORK ID: STFNET
  CONTROL POINT NAME: NN6
  XID: 00000
  APPN ENABLED: YES
  MAX SHARED MEMORY: 4096
  MAX CACHED: 4000
DLUR:
  DLUR ENABLED: YES
  PRIMARY DLUS NAME: NETB.MVSC
CONNECTION NETWORK:
  CN NAME          LINK TYPE  PORT INTERFACES
-----
COS:
  COS NAME
  -----
  BATCH
  BATCHSC
  CONNECT
  INTER
  INTERSC
  CPSVCMG
  SNASVCMG
  USRNOT
MODE:
  MODE NAME  COS NAME
  -----
  USRBAT    USRBAT
  USRNOT    USRNOT

PORT:
  INTF  PORT  LINK  HPR  SERVICE  PORT
  NUMBER NAME TYPE  ENABLED ANY  ENABLED
-----
  0     TR000  IBMTRNET  YES  YES  YES
  1     PPP001  PPP  YES  YES  YES
  2     SS      SDLC  NO   YES  YES
  3     SDLC  NO   YES  NO
  4     PPP  YES  YES  NO
  5     TR005  IBMTRNET  YES  YES  YES
  254   DLS  NO   YES  NO
  17    PPP017  PPP  YES  YES  YES

STATION:
  STATION  PORT  DESTINATION  HPR  ALLOW  ADJ  NODE
  NAME     NAME  ADDRESS      ENABLED  CP-CP  TYPE
-----
  TONN1    TR000  0004AC4E7505  YES  YES  1
  TONN2    TR000  550020004020  YES  YES  1
  TONN9    TR000  0004AC4E951D  YES  YES  1
  TOPC4    TR000  0004AC9416B4  YES  YES  1
  TOVTAM1  TR000  400000003888  YES  YES  1
  TONN35   PPP001  000000000000  YES  YES  0

LU NAME:
  LU NAME          STATION NAME          CP NAME
-----
APPN config>

```

Nota:

1 La ruta primaria es la interfaz 1, Frame Relay

- 2** La ruta alternativa es la interfaz 4 y está inhabilitada
- 3** El destino del redireccionamiento de la WAN es NN6
- 4** Configure el redireccionamiento primario y alternativo de la WAN
- 5** Añada el puerto APPN a NN22
- 6** Estación de enlace en el puerto APPN (NN22)
- 7** Puerto primario
- 8** Puerto alternativo
- 9** Estación alternativa con NN6
- 10** Estación primaria con NN6
- 11** Configuración de destino
- 12** Puerto APPN en destino; la estación de enlace se creará dinámicamente cuando se produzca el redireccionamiento de la WAN.

Configuración de la restauración de la WAN

El ejemplo siguiente muestra APPN sobre un enlace PPP primario. Para APPN, no se necesita ninguna definición única. Los dos extremos del enlace de comunicación están habilitados para la restauración de la WAN y están configurados de forma similar.

```
*****
*** Configuration of NN6 with a Wan Restoral link to NN35
*** interface 1 is the primary, interface 8 is the Secondary
*** NN35 must also have Wan Restoral configured for its primary/secondary
*** interfaces
**** Note that for APPN, there are NO unique definitions needed.
*****
```

Circuit configuration

FR Config>**li a1**

```
Base net                = 6
Destination name        = 2210-35
Circuit priority        = 8

Inbound destination name = 2210-35

Inbound calls           = allowed
Idle timer              = 0 (fixed circuit)
SelfTest Delay Timer    = 150 ms
```

FR Config>**ex**

Config>**fea wan**

WAN Restoral user configuration

WRS Config>**li a11**

```
WAN Restoral is enabled. 1
Default Stabilization Time: 0 seconds
Default First Stabilization Time: 0 seconds
```

```

Primary Interface      Secondary Interface    Secondary
-----
1 - WAN PPP           8 - PPP Dial Circuit   Enabled
[No Primary-Alternate pairs defined ]
WRS Config>ex
Config>p appn
APPN user configuration
APPN config>li al
NODE:
    NETWORK ID: STFNET
    CONTROL POINT NAME: NN6
    XID: 00000
    APPN ENABLED: YES
    MAX SHARED MEMORY: 4096
    MAX CACHED: 4000
DLUR:
    DLUR ENABLED: YES
    PRIMARY DLUS NAME: NETB.MVSC
CONNECTION NETWORK:
    CN NAME          LINK TYPE  PORT INTERFACES
-----
COS:
    COS NAME
-----
    BATCH
    BATCHSC
    CONNECT
    INTER
    INTERSC
    CPSVCMG
    SNASVCMG
USRBAT
USRNOT
MODE:
    MODE NAME  COS NAME
-----
    USRBAT    USRBAT
    USRNOT    USRNOT
PORT:
    INTF  PORT  LINK  HPR  SERVICE  PORT
    NUMBER NAME TYPE  ENABLED ANY  ENABLED
-----
    0      TR000  IBMTRNET  YES  YES  YES
**** < This is the port that will get backed up
    1      PPP001  PPP  YES  YES  YES  2
    2      SS      SDLC  NO   YES  YES
    3      SDLC  NO   YES  NO
    4      PPP  YES  YES  NO
    5      TR005  IBMTRNET  YES  YES  YES  YES
    254    DLS  NO   YES  NO
    17    PPP017  PPP  YES  YES  YES
    9      PPP009  PPP  YES  YES  YES
STATION:
    STATION  PORT  DESTINATION  HPR  ALLOW  ADJ NODE
    NAME     NAME  ADDRESS      ENABLED  CP-CP  TYPE
-----
    TONN1    TR000  0004AC4E7505  YES  YES  1
    TONN2    TR000  550020004020  YES  YES  1
    TONN9    TR000  0004AC4E951D  YES  YES  1
    TOPC4    TR000  0004AC9416B4  YES  YES  1
    TOVTAM1  TR000  400000003888  YES  YES  1
**** < this linkstation will get backed up
    TONN35   PPP001  000000000000  YES  YES  0  3
    T015D0D  PPP009  000000000000  YES  NO  0
LU NAME:
    LU NAME          STATION NAME          CP NAME
-----
APPN config>ex
Config>
*logout
Connection closed.

```

Nota:

- 1** La restauración de la WAN está habilitada en ambos extremos.
- 2** Puerto que tendrá seguridad
- 3** Estación de enlace que tendrá estación de reserva

Configuración de V.25 bis

A continuación se muestra un ejemplo de configuración de V.25 bis que puede usarse cuando el tráfico APPN utiliza PPP sobre V.25 bis :

```
Config> list device
Ifc 0 Token Ring          CSR 6000000, vector 28
Ifc 1 WAN PPP             CSR 81620, CSR2 80D00, vector 93
Ifc 2 WAN V.25bis        CSR 81640, CSR2 80E00, vector 92
```

```
Config>set data v25 2.
Config>list device
Ifc 0 Token Ring          CSR 6000000, vector 28
Ifc 1 WAN PPP             CSR 81620, CSR2 80D00, vector 93
Ifc 2 WAN V.25bis        CSR 81640, CSR2 80E00, vector 92
```

```
Config>add v25
Assign address name (1-23) chars []? brown
Assign network dial address (1-30 digits) []? 555-1211
Assign address name (1-23) chars []? gray
Assign network dial address (1-30 digits) []? 555-1212
Config>list v25
```

Address assigned name	Network Address
-----	-----
brown	555-1211
gray	555-1212

```
Config>add device dial
Adding device as interface 3
Defaulting Data-link protocol to PPP
Use net 3 command to configure circuit parameters
Config>net 3
Circuit configuration
Circuit config: 3>list all.
```

```
Base net                = 0
Destination name        =
Circuit priority        = 8

Outbound calls          = allowed
Inbound calls           = allowed
Idle timer              = 60 sec 1
SelfTest Delay Timer    = 150 ms
```

```
Circuit config: 3>set net
Base net for this circuit [0]? 2
Circuit config: 3>set idle 0 2
Circuit config: 3>set dest
Assign destination address name []? brown
```

```
Circuit config: 3>list all

Base net                = 2
Destination name       = brown
Circuit priority       = 8
Destination address: subaddress = 555-1211

Outbound calls         = allowed
Inbound calls          = allowed
Idle timer             = 0 (fixed circuit)
SelfTest Delay Timer   = 150 ms

Circuit config: 3>ex
Config>net 2
V.25bis Data Link Configuration
V25bis Config>list all
    V.25bis Configuration
Local Network Address Name = Unassigned
No local addresses configured

Non-Responding addresses:
Retries                 = 1
Timeout                 = 0 seconds

Call timeouts:
Command Delay           = 0 ms
Connect                 = 60 seconds
Disconnect               = 2 seconds

Cable type              = RS-232 DTE

Speed (bps)             = 9600
V25bis Config>set local
Local network address name []? gray
V25bis Config>list all
    V.25bis Configuration
Local Network Address Name = gray
Local Network Address     = 555-1212

Non-Responding addresses:
Retries                 = 1
Timeout                 = 0 seconds

Call timeouts:
Command Delay           = 0 ms
Connect                 = 60 seconds
Disconnect               = 2 seconds

Cable type              = RS-232 DTE

Speed (bps)             = 9600
V25bis Config>
```

Nota:

- 1** Un valor que no es cero para el temporizador de desocupación da como resultado un enlace de marcación bajo pedido
- 2** Un valor cero da como resultado un enlace alquilado

Configuración de V.34

A continuación, se muestra un ejemplo de configuración de V.34 que puede usarse cuando el tráfico APPN usa PPP sobre V.34:

```

Config>list device
Ifc 0 Token Ring          CSR 6000000, vector 28
Ifc 1 WAN PPP            CSR 81620, CSR2 80D00, vector 93
Ifc 2 WAN PPP            CSR 81640, CSR2 80E00, vector 92
Config>set data v34 2. Config>list device
Ifc 0 Token Ring          CSR 6000000, vector 28
Ifc 1 WAN PPP            CSR 81620, CSR2 80D00, vector 93
Ifc 2 V.34 Base Net      CSR 81640, CSR2 80E00, vector 92
Config>add v34
Assign address name [1-23] chars []? brown
Assign network dial address [1-30 digits] []? 555-1211
Config>add v34
Assign address name [1-23] chars []? gray
Assign network dial address [1-30 digits] []? 555-1212
Config>list v34

Address assigned name      Network Address
-----
default_address           9999999
brown                     555-1211
gray                      555-1212
Config>add device dial
Adding device as interface 3
Defaulting Data-link protocol to PPP
Use "net 3" command to configure circuit parameters
Config>net 3
Circuit configuration
Circuit config: 3>list all.

Base net                   = 0
Destination name           =
Circuit priority           = 8

Outbound calls             = allowed
Inbound calls              = allowed
Idle timer                 = 60 sec
SelfTest Delay Timer       = 150 ms

Circuit config: 3>set net
Base net for this circuit [0]? 2
Circuit config: 3>set idle 0
Circuit config: 3>set dest
Assign destination address name []? brown

```

```
Circuit config: 3>list all
```

```
Base net = 2
Destination name = brown
Circuit priority = 8
Destination address: subaddress = 555-1211

Outbound calls = allowed
Inbound calls = allowed
Idle timer = 0 (fixed circuit)
SelfTest Delay Timer = 150 ms
```

```
Circuit config: 3>ex
Config>net 2
V.34 Data Link Configuration
V.34 System Net Config 2>list all
```

V.34 System Net Configuration:

```
Local Network Address Name = default_address
Local Network Address = 9999999
```

```
Non-Responding addresses:
Retries = 1
Timeout = 0 seconds
```

```
Call timeouts:
Command Delay = 0 ms
Connect = 60 seconds
Disconnect = 2 seconds
```

```
Modem strings:
Initialization string = at&f&s111&d2&c1x3
Speed (bps) = 115200
```

```
V.34 System Net Config 2>set local
Local network address name []? gray
V.34 System Net Config 2>list all
```

V.34 System Net Configuration:

```
Local Network Address Name = gray
Local Network Address = 555-1212
```

```
Non-Responding addresses:
Retries = 1
Timeout = 0 seconds
```

```
Call timeouts:
Command Delay = 0 ms
Connect = 60 seconds
Disconnect = 2 seconds
```

```
Modem strings:
Initialization string = at&f&s111&d2&c1x3
```

```
Speed (bps) = 115200
```

```
V.34 System Net Config 2>
```

Notas:

- 1** Un valor que no es cero para el temporizador de desocupación da como resultado un enlace de marcación bajo pedido
- 2** Un valor cero da como resultado un enlace alquilado

Configuración de APPN sobre ATM

En el ejemplo siguiente se muestra una configuración de APPN sobre ATM.

Notas:

1. Cuando se configuran PVC, debe definirse la estación de enlace en los dos nodos de APPN que deseen utilizar el PVC. La estación de enlace debe estar definida con **Activate link automatically** = yes (Activar enlace automáticamente = sí).
2. Cuando se configuran TG paralelos sobre ATM, el nombre del nodo adyacente y el número de TG deben estar definidos en los dos nodos de cada estación de enlace.

Nota: Al definir TG paralelos si se utiliza la asignación de números de TG dinámica, deben definirse TODOS o NINGUNO de los enlaces entre los dos nodos.

```

add po
APPN Port
Link Type: (P)PP, (FR)AME RELAY, (E)THERNET, (T)OKEN RING,
(S)DLC, (X)25, (D)LSw,(A)TM, (IP) [ ]?atm 1
Interface number(Default 0): [0]?6
Port name (Max 8 characters) [ATM006]?

WARNING!! You are changing an existing record.
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
  Service any node: (Y)es (N)o [Y]?
  Maximum BTU size (768-2048) [2048]?
  Percent of link stations reserved for incoming calls (0-100) [0]?
  Percent of link stations reserved for outgoing calls (0-100) [0]?
  Local ATM Address (hex) [99998888777766]?
  Local SAP address (04-EC) [4]?
  Enable Incoming Calls (Y)es (N)o [N]?
  ATM Network Type: 0 = CAMPUS, 1 = WIDEAREA [0]?
  Shareable Connection Network Traffic (Y)es (N)o [N]?
  Shareable Other Protocol Traffic (Y)es (N)o [N]?
  Broadband Bearer Class: 0 = CLASS_A, 1 = CLASS_C, 2 = CLASS_X [2]?
  Best Effort Indicator (Y)es (N)o [N]?
  Forward Traffic Peak Cell Rate (1-16777215) [131750]?
  Forward Traffic Sustained Cell Rate (1-16777215) [131750]?
  Forward Traffic Tagging (Y)es (N)o [Y]?
  Forward Traffic QOS Class: 0 = CLASS_0, 1 = CLASS_1, 2 = CLASS_2,
  3 = CLASS_3, 4 = CLASS_4 [0]?
  Backward Traffic Peak Cell Rate (1-16777215) [460800]?
  Backward Traffic Sustained Cell Rate (1-16777215) [39168]?
  Backward Traffic Tagging (Y)es (N)o [Y]?
  Backward Traffic QOS Class: 0 = CLASS_0, 1 = CLASS_1, 2 = CLASS_2,
  3 = CLASS_3, 4 = CLASS_4 [0]?
  Call out anonymously (Y)es (N)o [N]?
  LDLC Retry Count(1-255) [3]?
  LDLC Timer Period(1-255 seconds) [1]?
  Limited resource timer for HPR(1-2160000 seconds) [180]?
Would you like TG characteristics updated to recommended
values based on config changes: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y ] ?
The record has been written.

```

```
nada205 APPN config>add li atm006 2
APPN Station
Station name (Max 8 characters) [ ]?tograya
WARNING!! You are changing an existing record.
Limited resource: (Y)es (N)o[N]?
Activate link automatically (Y)es (N)o[Y]?
Virtual Channel Type (0 = PVC , 1 = SVC) [0]? 3
Destination ATM Address [39999999999900009999010103168902259411]?
VPI (0-255) [0]?
VCI (0-65535) [70]? 34
ATM Network Type: 0 = CAMPUS, 1 = WIDEAREA [0]?
Shareable Connection Network Traffic (Y)es (N)o [N]?
Shareable Other Protocol Traffic (Y)es (N)o [N]?
Remote SAP(04-EC) [4]?
Adjacent node type: 0 = APPN network node,
1 = APPN end node or Unknown node type,
2 = LEN end node [0]?
Allow CP-CP sessions on this link (Y)es (N)o [Y]?
CP-CP session level security (Y)es (N)o [N]?
Configure CP name of adjacent node: (Y)es (N)o [N]?
LDLC Retry Count(1-255) [3]?
LDLC Timer Period(1-255 seconds) [1]?
Would you like TG characteristics updated to recommended
values based on config changes: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y ] ?
The record has been written.
```

```
nada205 APPN config>add link atm006
APPN Station
Station name (Max 8 characters) [ ]?tograya
WARNING!! You are changing an existing record.
Limited resource: (Y)es (N)o[N]?
Activate link automatically (Y)es (N)o[Y]?
Virtual Channel Type (0 = PVC , 1 = SVC) [0]? 1 4
Destination ATM Address [39999999999900009999010103168902259411]?
Broadband Bearer Class: 0 = CLASS_A, 1 = CLASS_C, 2 = CLASS_X [2]?
Best Effort Indicator (Y)es (N)o [N]?
Forward Traffic Peak Cell Rate (1-16777215) [30000]?
Forward Traffic Sustained Cell Rate (1-16777215) [20000]?
Forward Traffic Tagging (Y)es (N)o [Y]?
Forward Traffic QOS Class: 0 = CLASS_0, 1 = CLASS_1, 2 = CLASS_2,
3 = CLASS_3, 4 = CLASS_4 [0]?
Backward Traffic Peak Cell Rate (1-16777215) [30000]?
Backward Traffic Sustained Cell Rate (1-16777215) [20000]?
Backward Traffic Tagging (Y)es (N)o [Y]?
Backward Traffic QOS Class: 0 = CLASS_0, 1 = CLASS_1, 2 = CLASS_2,
3 = CLASS_3, 4 = CLASS_4 [0]?
Call out anonymously (Y)es (N)o [N]?
ATM Network Type: 0 = CAMPUS, 1 = WIDEAREA [0]?
Shareable Connection Network Traffic (Y)es (N)o [N]?
Shareable Other Protocol Traffic (Y)es (N)o [N]?
Remote SAP(04-EC) [4]?
Adjacent node type: 0 = APPN network node,
1 = APPN end node or Unknown node type,
2 = LEN end node [0]?
TG Number (0-20) [0]?
Allow CP-CP sessions on this link (Y)es (N)o [Y]?
CP-CP session level security (Y)es (N)o [N]?
Configure CP name of adjacent node: (Y)es (N)o [N]?
LDLC Retry Count(1-255) [3]?
LDLC Timer Period(1-255 seconds) [1]?
Would you like TG characteristics updated to recommended
values based on config changes: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y ] ?
The record has been written.
```

```
nada205 APPN config>
```


Notas:

- 1** Defina un puerto APPN con el tipo de enlace ATM
- 2** Defina una estación de enlace de APPN
- 3** Defina un PVC
- 4** Defina un SVC

Configuración de APPN usando SDLC

APPN da soporte a la estaciones de SDLC siguientes:

- Primaria de punto a punto
- Secundaria de punto a punto
- Negociable de punto a punto
- Primaria multipunto
- Secundaria de punto a punto (diversas estaciones de enlace de APPN)

Con la interfaz de mandatos **talk 5** para SDLC, puede:

- Habilitar/inhabilitar un enlace SDLC
- Actualizar los parámetros de estación de SDLC

Para activar una conexión APPN con la estación de enlace SDLC remota, deberá configurar y activar la estación de enlace de APPN SDLC en el direccionador. Esto habilitará a la estación de enlace de APPN del direccionador para recibir un XID de activación de la estación de enlace remota SDLC. Esto es diferente de otros tipos de DLC como, por ejemplo, la red en anillo o Ethernet, cuyas estaciones de enlace de APPN no necesitan estar definidas explícitamente para APPN en el direccionador, ya que APPN tiene la posibilidad de definir dinámicamente estos tipos de estaciones de enlace.

Consulte el manual Guía del usuario de software para obtener información adicional sobre la configuración de capas de la red SDLC.

```

*****
*
* Los ejemplos siguientes muestran cómo configurar estaciones SDLC
diferentes.
*
*****
*Configuring a Primary Point-To-Point SDLC Station: 1
*****
Config> set data sdlc 1
Config> n 1
SDLC user configuration
SDLC 1 Config> set link role primary
SDLC 1 Config>list link
list link
Link configuration for: LINK_1 (ENABLED)

Role:          PRIMARY          Type:          POINT-TO-POINT
Duplex:        FULL             Modulo:        8
Idle state:    FLAG             Encoding:       NRZ
Clocking:      INTERNAL         Frame Size:    2048
Speed:         64000            Group Poll:    00
Cable:         RS-232 DCE

Timers:        XID/TEST response: 2.0 sec
                SNRM response:    2.0 sec
                Poll response:     0.5 sec
                Inter-poll delay:  0.2 sec
                RTS hold delay:     DISABLED
                Inter-frame delay:  DISABLED
                Inactivity timeout: 30.0 sec

Counters:      XID/TEST retry:  8
                SNRM retry:       6
                Poll retry:        10

SDLC 1 Config>ex
Config> CTRL p
* restart
Are you sure you want to restart the gateway? (Yes or [No]): yes

* t 6
Config>p appn
APPN user configuration
APPN config>add port sdlc
APPN Port
Interface number(Default 0): [0]? 1
Port name (Max 8 characters) [SDLC001]?
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
    Service any node: (Y)es (N)o[Y]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y ] ?
The record has been written.

```

```

APPN config>list port sdlc001
PORT:
  Interface number(DLSw = 254): 1
    PORT enable: YES
    Service any node: YES
  Link Type: SDLC
    MAX BTU size: 2048
  MAX number of Link Stations: 1
    Percent of link stations reserved for incoming calls: 0
    Percent of link stations reserved for outgoing calls: 0
    Cost per connect time: 0
    Cost per byte: 0
    Security:(0 = Nonsecure, 1 = Public Switched Network
      2 = Underground Cable, 3 = Secure Conduit,
      4 = Guarded Conduit, 5 = Encrypted, 6 = Guarded Radiation): 0
    Propagation delay:(0 = Minimum, 1 = Lan, 2 = Telephone,
      3 = Packet Switched Network, 4 = Satellite, 5 = Maximum): 2
    Effective capacity: 45
    First user-defined TG characteristic: 128
    Second user-defined TG characteristic: 128
    Third user-defined TG characteristic: 128
APPN config>add link sdlc001
APPN Station
Station name (Max 8 characters) [ ]? TOSECSTN
  Activate link automatically (Y)es (N)o[Y]?
  Station address(1-fe) [C1]?
  Adjacent node type: 0 = APPN network node, 1 = APPN end node
  2 = LEN end node, 3 = PU 2.0 node [0]?
Edit Dependent LU Server: (Y)es (N)o [N]?
  Allow CP-CP sessions on this link (Y)es (N)o [Y]?
  CP-CP session level security (Y)es (N)o [N]?
  Configure CP name of adjacent node: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y ] ?
The record has been written.

APPN config>list link tosecstn
STATION:
  Port name: SDLC001
  Interface number(DLSw = 254): 1
  Link Type: SDLC
  Station address: C1
    Activate link automatically: YES
    Allow CP-CP sessions on this link: YES
    CP-CP session level security: NO
    Fully-qualified CP name of adjacent node:
    Encryption key: 0000000000000000
    Use enhanced session security only: NO
    Cost per connect time: 0
    Cost per byte: 0
    Security:(0 = Nonsecure, 1 = Public Switched Network
      2 = Underground Cable, 3 = Secure Conduit,
      4 = Guarded Conduit, 5 = Encrypted, 6 = Guarded Radiation): 0
    Propagation delay:(0 = Minimum, 1 = Lan, 2 = Telephone,
      3 = Packet Switched Network, 4 = Satellite, 5 = Maximum): 2
    Effective capacity: 45
    First user-defined TG characteristic: 128
    Second user-defined TG characteristic: 128
    Third user-defined TG characteristic: 128
    Predefined TG number: 0
APPN config>act
*****
* Configuring a Secondary Point-To-Point SDLC Station: 2
*****
Config> set data sdlc 1
Config> n 1
SDLC user configuration
SDLC 1 Config> set link role secondary
SDLC 1 Config> set link cable rs-232 dte
SDLC 1 Config>list link      **(will show
link configuration)

```

```

SDLC 1 Config>add station
Enter station address (in hex) [C1]?
Enter station name [SDLC_C1]?
Include station in group poll list ([Yes] or No): no
Enter max packet size [2048]?
Enter receive window [7]?
Enter transmit window [7]?
SDLC 1 Config>list station all
Address      Name      Status    Max BTU  Rx Window  Tx Window
-----
   C1      SDLC_C1  ENABLED      2048      7          7
SDLC 1 Config>ex
Config> CTRL p
* restart
Are you sure you want to restart the gateway? (Yes or [No]): yes

* t 6
Config>p appn
APPN user configuration
APPN config>add port sdlc
APPN Port
Interface number(Default 0): [0]? 1
Port name (Max 8 characters) [SDLC001]?
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
    Service any node: (Y)es (N)o[Y]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y ] ?
The record has been written.
APPN config>list port sdlc001  **(will show port definitions)
APPN config>add link sdlc001
APPN Station
Station name (Max 8 characters) [ ]? TOPRISTN
    Activate link automatically (Y)es (N)o[Y]?
(Note: "Y" to accept activation from the primary or negotiable station)
Station address(1-fe) [C1]?
Adjacent node type: 0 = APPN network node, 1 = APPN end node
                2 = LEN end node, 3 = PU 2.0 node [0]?
Edit Dependent LU Server: (Y)es (N)o [N]?
    Allow CP-CP sessions on this link (Y)es (N)o [Y]?
    CP-CP session level security (Y)es (N)o [N]?
    Configure CP name of adjacent node: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y ] ?
The record has been written.

```

```

APPN config>list link topristn ** (will show link station definitions)
APPN config>act
*****
* Configuring a Negotiable Point-To-Point SDLC Station: 3
*****
Config> set data sdlc 1
Config> n 1
SDLC user configuration
SDLC 1 Config> set link role negotiable
SDLC 1 Config>list link ** (will show
link configuration)
SDLC 1 Config>ex
Config> CTRL p
* restart
Are you sure you want to restart the gateway? (Yes or [No]): yes

* t 6
Config>p appn
APPN user configuration
APPN config>add port sdlc
APPN Port
Interface number(Default 0): [0]? 1
Port name (Max 8 characters) [SDLC001]?
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
    Service any node: (Y)es (N)o [Y]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y ] ?
The record has been written.
APPN config>list port sdlc001 ** (will show port definitions)
APPN config>add link sdlc001
APPN Station
Station name (Max 8 characters) [ ]? TOREMSTN
    Activate link automatically (Y)es (N)o [Y]?
Station address(1-fe) [C1]?
(Note: C1 may be used if this station is becoming a secondary station)
Adjacent node type: 0 = APPN network node, 1 = APPN end node
2 = LEN end node, 3 = PU 2.0 node [0]?
Edit Dependent LU Server: (Y)es (N)o [N]?
    Allow CP-CP sessions on this link (Y)es (N)o [Y]?
    CP-CP session level security (Y)es (N)o [N]?
    Configure CP name of adjacent node: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y ] ?
The record has been written.

```

```

APPN config>list link toremstn  **(mostrará las definiciones de
estaciones de enlace)
APPN config>act
*****
* Configuring a Primary Multipoint SDLC Station:  4
*****
Config> set data sdlc 1
Config> n 1
SDLC user configuration
SDLC 1 Config> set link role primary
SDLC 1 Config> set link type multipoint
SDLC 1 Config>list link          **(will show
link configuration)
SDLC 1 Config>ex
Config> CTRL p
* reload
Are you sure you want to reload the gateway? (Yes or [No]): yes
* t 6
Config>p appn
APPN user configuration
APPN config>add port sdlc
APPN Port
Interface number(Default 0): [0]? 1
Port name (Max 8 characters) [SDLC001]?
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
    Service any node: (Y)es (N)o[Y]?
    Maximum number of link stations (1-127) ? 2
    Edit TG Characteristics: (Y)es (N)o [N]?
    Write this record? [Y ] ?
    The record has been written.
APPN config>list port sdlc001          **(will show port definitions)
APPN config>add link sdlc001
APPN Station
Station name (Max 8 characters) [ ]? TOSTNC1
    Activate link automatically (Y)es (N)o[Y]?
    Station address(1-fe) [C1]?
    (Note: C1 must match to the remote secondary station)
    Adjacent node type: 0 = APPN network node, 1 = APPN end node
    2 = LEN end node, 3 = PU 2.0 node [0]?
    Edit Dependent LU Server: (Y)es (N)o [N]?
        Allow CP-CP sessions on this link (Y)es (N)o [Y]?
        CP-CP session level security (Y)es (N)o [N]?
        Configure CP name of adjacent node: (Y)es (N)o [N]?
    Edit TG Characteristics: (Y)es (N)o [N]?
    Write this record? [Y ] ?
    The record has been written.
APPN config>list link tostnc1          **(will show link station definitions)
APPN config>add link sdlc001
APPN Station
Station name (Max 8 characters) [ ]?
TOSTNC2
    Activate link automatically (Y)es (N)o[Y]?
    Station address(1-fe) [C2]?
    (Note: C2 must match to the remote secondary station)
    Adjacent node type: 0 = APPN network node, 1 = APPN end node
    2 = LEN end node, 3 = PU 2.0 node [0]?
    Edit Dependent LU Server: (Y)es (N)o [N]?
        Allow CP-CP sessions on this link (Y)es (N)o [Y]?
        CP-CP session level security (Y)es (N)o [N]?
        Configure CP name of adjacent node: (Y)es (N)o [N]?
    Edit TG Characteristics: (Y)es (N)o [N]?
    Write this record? [Y ] ?
    The record has been written.
APPN config>list link tostnc2  **(mostrará definiciones de estaciones de enlace)
APPN config>act

```

```

*****
* Configuring a Secondary point-to-point (Multi APPN link station): 5
*****
Config> set data sdlc 1
Config> n 1
SDLC user configuration
SDLC 1 Config> set link role secondary
SDLC 1 Config> set link type point-to-point
SDLC 1 Config>list link          **(will show
link configuration)
SDLC 1 Config>ex
Config> CTRL p
* reload
Are you sure you want to reload the gateway? (Yes or [No]): yes
* t 6
Config>p appn
APPN user configuration
APPN config>add port sdlc
APPN Port
Interface number(Default 0): [0]? 1
Port name (Max 8 characters) [SDLC001]?
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
    Service any node: (Y)es (N)o[Y]?
    Maximum number of link stations (1-127) ? 2
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y ] ?
The record has been written.
APPN config>list port sdlc001          **(will show port definitions)
APPN config>add link sdlc001
APPN Station
Station name (Max 8 characters) [ ]? TOSTNC1
    Activate link automatically (Y)es (N)o[Y]?
    Station address(1-fe) [C1]?
    (Note: C1 must match to the remote secondary station)
    Adjacent node type: 0 = APPN network node, 1 = APPN end node
    2 = LEN end node, 3 = PU 2.0 node [0]?
Edit Dependent LU Server: (Y)es (N)o [N]?
    Allow CP-CP sessions on this link (Y)es (N)o [Y]?
    CP-CP session level security (Y)es (N)o [N]?
    Configure CP name of adjacent node: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y ] ?
The record has been written.
APPN config>list link tostnc1          **(will show link station definitions)
APPN config>add link sdlc001
APPN Station
Station name (Max 8 characters) [ ]?
TOSTNC2
    Activate link automatically (Y)es (N)o[Y]?
    Station address(1-fe) [C2]?
    (Note: C2 must match to the remote secondary station)
    Adjacent node type: 0 = APPN network node, 1 = APPN end node
    2 = LEN end node, 3 = PU 2.0 node [0]?
Edit Dependent LU Server: (Y)es (N)o [N]?
    Allow CP-CP sessions on this link (Y)es (N)o [Y]?
    CP-CP session level security (Y)es (N)o [N]?
    Configure CP name of adjacent node: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y ] ?
The record has been written.
APPN config>list link tostnc2          **(mostrará definiciones de estaciones de enlace)
APPN config>act

```

Nota:

- 1** Configuración de una estación SDLC primaria de punto a punto
- 2** Configuración de una estación SDLC secundaria de punto a punto
- 3** Configuración de una estación SDLC negociable de punto a punto
- 4** Configuración de una estación SDLC multipunto primaria
- 5** Configuración secundaria de punto a punto (diversas estaciones de enlace de APPN)

Configuración de APPN sobre X.25

Este ejemplo muestra la configuración de APPN sobre un puerto X.25 y dos estaciones de enlace. Una de ellas es un PVC y otra un SVC. El SVC está configurado como recurso limitado. El SVC se activará cuando sea necesario y se desactivará cuando no lo sea.

```
Boats Config>p appn
APPN user configuration
Boats APPN config>add port
APPN Port
Link Type: (P)PP, (F)RAME RELAY, (E)THERNET, (T)OKEN RING,
(S)DLC, (X)25, (D)LSw, (A)TM, (IP)[ ]? x
Interface number(Default 0):[0]? 2
Port name (Max 8 characters)[X25002]?
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
Service any node: (Y)es (N)o[Y]?
Maximum number of link stations (1-65535)[65535]?
Percent of link stations reserved for incoming calls (0-100) [0]?
Percent of link stations reserved for outgoing calls (0-100) [0]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y ] ?
The record has been written.

Boats APPN config>add link
APPN Station
Port name for the link station[ ]? x25002
Station name (Max 8 characters)[ ]? x25svc1
Limited resource: (Y)es (N)o[N]? Y
Activate link automatically (Y)es (N)o[N]?
Link Type (0 = PVC , 1 = SVC)[0]? 1
DTE Address [0]? 2222
Adjacent node type: 0 = APPN network node,
1 = APPN end node or Unknown node type
2 = LEN end node, 3 = PU 2.0 node[1]?
Edit Dependent LU Server: (Y)es (N)o [N]?
Allow CP-CP sessions on this link (Y)es (N)o[Y]? N
CP-CP session level security (Y)es (N)o [N]?
Configure CP name of adjacent node: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y ] ?
The record has been written.

Boats APPN config>add link
APPN Station
Port name for the link station[ ]? x25002
Station name (Max 8 characters)[ ]? x25pvc1
Limited resource: (Y)es (N)o[N]?
Activate link automatically (Y)es (N)o[Y]?
Link Type (0 = PVC , 1 = SVC)[0]?
Logical channel number (1-4095)[1]?
Adjacent node type: 0 = APPN network node,
1 = APPN end node or Unknown node type
2 = LEN end node, 3 = PU 2.0 node[1]?
```



```

Edit Dependent LU Server: (Y)es (N)o [N]?
    Allow CP-CP sessions on this link (Y)es (N)o [Y]?
    CP-CP session level security (Y)es (N)o [N]?
    Configure CP name of adjacent node: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y ] ?
The record has been written.
Boats APPN config>list port x25002
PORT:
    Interface number(DLSw = 254): 2
    PORT enable: YES
    Service any node: YES
    Link Type: X25
    MAX BTU size: 2048
    MAX number of Link Stations: 239
    Percent of link stations reserved for incoming calls: 0
    Percent of link stations reserved for outgoing calls: 0
    Cost per connect time: 0
    Cost per byte: 0
    Security:(0 = Nonsecure, 1 = Public Switched Network
        2 = Underground Cable, 3 = Secure Conduit,
        4 = Guarded Conduit, 5 = Encrypted, 6 = Guarded Radiation): 0
    Propagation delay:(0 = Minimum, 1 = Lan, 2 = Telephone,
        3 = Packet Switched Network, 4 = Satellite, 5 = Maximum): 3
    Effective capacity: 45
    First user-defined TG characteristic: 128
    Second user-defined TG characteristic: 128
    Third user-defined TG characteristic: 128
Boats APPN config>list link x25svcl1
STATION:
    Port name: X25002
    Interface number(DLSw = 254): 2
    Link Type: X25
    Link Type (0 = PVC , 1 = SVC): 1
    DTE Address: 2222
    Activate link automatically: YES
    Allow CP-CP sessions on this link: YES
    CP-CP session level security: NO
    Fully-qualified CP name of adjacent node:
    Encryption key: 0000000000000000
    Use enhanced session security only: NO
    Cost per connect time: 0
    Cost per byte: 0
    Security:(0 = Nonsecure, 1 = Public Switched Network
        2 = Underground Cable, 3 = Secure Conduit,
        4 = Guarded Conduit, 5 = Encrypted, 6 = Guarded Radiation): 0
    Propagation delay:(0 = Minimum, 1 = Lan, 2 = Telephone,
        3 = Packet Switched Network, 4 = Satellite, 5 = Maximum): 3
    Effective capacity: 45
    First user-defined TG characteristic: 128
    Second user-defined TG characteristic: 128
    Third user-defined TG characteristic: 128
    Predefined TG number: 0

```

```

Boats APPN config>list link x25pvc1
STATION:
  Port name: X25002
  Interface number(DLSw = 254): 2
  Link Type: X25
  Link Type (0 = PVC , 1 = SVC): 0
  Logical Channel number: 1
  Activate link automatically: YES
  Allow CP-CP sessions on this link: YES
  CP-CP session level security: NO
  Fully-qualified CP name of adjacent node:
  Encryption key: 0000000000000000
  Use enhanced session security only: NO
  Cost per connect time: 0
  Cost per byte: 0
  Security:(0 = Nonsecure, 1 = Public Switched Network
    2 = Underground Cable, 3 = Secure Conduit,
    4 = Guarded Conduit, 5 = Encrypted, 6 = Guarded Radiation): 0
  Propagation delay:(0 = Minimum, 1 = Lan, 2 = Telephone,
    3 = Packet Switched Network, 4 = Satellite, 5 = Maximum): 3
  Effective capacity: 45
  First user-defined TG characteristic: 128
  Second user-defined TG characteristic: 128
  Third user-defined TG characteristic: 128
  Predefined TG number: 0
Boats APPN config>li all
NODE:
  NETWORK ID: STFNET
  CONTROL POINT NAME: BOATS
  XID: 00000
  APPN ENABLED: YES
  MAX SHARED MEMORY: 4096
  MAX CACHED: 4000
DLUR:
  DLUR ENABLED: NO
  PRIMARY DLUS NAME:
CONNECTION NETWORK:
  CN NAME          LINK TYPE  PORT INTERFACES
-----
COS:
  COS NAME
  -----
  BATCH
  BATCHSC
  CONNECT
  INTER
  INTERSC
  CPSVCMG
  SNASVCMG
  MODE NAME  COS NAME
  -----

```

```

PORT:
      INTF   PORT   LINK   HPR   SERVICE   PORT
      NUMBER NAME   TYPE   ENABLED ANY   ENABLED
-----
       2   X25002   X25    NO    YES    YES
       5   TR005   IBMTRNET YES    YES    YES

STATION:
      STATION  PORT   DESTINATION   HPR   ALLOW   ADJ NODE
      NAME     NAME   ADDRESS       ENABLED CP-CP   TYPE
-----
      X25SVC1  X25002   2222         NO    NO     1
      X25PVC1  X25002   1            NO    YES    1

LU NAME:
      LU NAME   STATION NAME   CP NAME
-----

```

Boats APPN config>ex

```

Boats Config>n 2
X.25 User Configuration
Boats X.25 Config>li all

```

X.25 Configuration Summary

```

Node Address:      1111
Max Calls Out:    4
Inter-Frame Delay: 0   Encoding: NRZ
Speed:            64000   Clocking: External
MTU:              2048   Cable: V.35 DTE
Lower DTR:        Disabled
Default Window:   2     SVC idle: 30 seconds
National Personality: GTE Telenet (DCE)
PVC               low: 1   high: 4
Inbound           low: 0   high: 0
Two-Way           low: 10  high: 20
Outbound          low: 0   high: 0
Throughput Class in bps Inbound: 2400
Throughput Class in bps Outbound: 2400

```

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: off  Flow Control Negotiation: off
Suppress Calling Addresses: off
DDN Address Translation: 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: 10 seconds
T1 Timer: 4.00 seconds   N2 timeouts: 20
T2 Timer: 0.00 seconds   DP Timer: 500 milliseconds
Standard Version: 2     Network Type: CCITT
Disconnect Procedure: passive
Window Size   Frame: 7   Packet: 2
Packet Size   Default: 128   Maximum: 256

```

X.25 protocol configuration

Prot Number	Window Size	Packet-size Default	Packet-size Maximum	Idle Time	Max VCs	Station Type
30 -> APPN	7	128	1024	0	4	PEER

X.25 PVC configuration

Prtcl	X.25_address	Active Enc	Window	Pkt_len	Pkt_chan
30 (APPN)	6666	NONE	2	128	1

X.25 address translation configuration

IF #	Prot #	Active Enc	Protocol	-> X.25 address
2	30 (APPN)	NONE	appn	-> 6666

Boats X.25 Config>

Configuración de APPN sobre Frame Relay

El ejemplo siguiente muestra la configuración de APPN sobre Frame Relay.

```
nada207 Config>p appn
APPN user configuration
nada207 APPN config>add port
APPN Port
Link Type: (P)PP, (F)RAME RELAY, (E)THERNET, (T)OKEN RING,
(S)DLC, (X)25, (D)LSw, (A)TM, (IP) [ ] ?f
Interface number(Default 0): [0]? 4
Port name (Max 8 characters) [FR004]?
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
  Service any node: (Y)es (N)o [Y]?
  High performance routing: (Y)es (N)o [Y]?
  Maximum BTU size (768-2048) [2048]?
  Percent of link stations reserved for incoming calls (0-100) [0]?
  Percent of link stations reserved for outgoing calls (0-100) [0]?
  Local SAP address (04-EC) [4]?
  Support bridged formatted frames: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
nada207 APPN config>add link
APPN Station
Port name for the link station []? fr004
Station name (Max 8 characters) []? tonn
  Activate link automatically (Y)es (N)o [Y]?
  DLCI number for link (16-1007) [16]?
  Adjacent node type: 0 = APPN network node,
  1 = APPN end node or Unknown node type
  2 = LEN end node, 3 = PU 2.0 node [1]? 0
  High performance routing: (Y)es (N)o [Y]?
Edit Dependent LU Server: (Y)es (N)o [N]?
  Allow CP-CP sessions on this link (Y)es (N)o [Y]?
  CP-CP session level security (Y)es (N)o [N]?
  Configure CP name of adjacent node: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
nada207 APPN config>act
nada207 APPN config>exit
nada207 Config>write
Config Save: Using bank B and config number 2
```

Configuración de APPN sobre Frame Relay BAN

El ejemplo siguiente muestra la configuración de APPN sobre Frame Relay BAN.

```
nada207 Config>p appn
APPN user configuration
nada207 APPN config>add port
APPN Port
Link Type: (P)PP, (F)RAME RELAY, (E)THERNET, (T)OKEN RING,
(S)DLC, (X)25, (D)LSw, (A)TM, (IP) [ ] ?f
Interface number(Default 0): [0]? 4
Port name (Max 8 characters) [FR004]?
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
Service any node: (Y)es (N)o [Y]?
High performance routing: (Y)es (N)o [Y]?
Maximum BTU size (768-2048) [2048]?
Percent of link stations reserved for incoming calls (0-100) [0]?
Percent of link stations reserved for outgoing calls (0-100) [0]?
Local SAP address (04-EC) [4]?
Support bridged formatted frames: (Y)es (N)o [N]? y
Boundary node identifier (hex-noncanonical) [4FFF00000000]?
41235fad
Local HPR SAP address (04-EC) [C8]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
nada207 APPN config> add link
APPN Station
Port name for the link station []? fr004
Station name (Max 8 characters) []? tonn
Activate link automatically (Y)es (N)o [Y]?
DLCI number for link (16-1007) [16]?
Support bridged formatted frames: (Y)es (N)o [N]? y
MAC address of adjacent node (hex-noncanonical) [000000000000]? 3456
Adjacent node type: 0 = APPN network node,
1 = APPN end node or Unknown node type
2 = LEN end node, 3 = PU 2.0 node [1]? 0
High performance routing: (Y)es (N)o [Y]?
Edit Dependent LU Server: (Y)es (N)o [N]?
Allow CP-CP sessions on this link (Y)es (N)o [Y]?
CP-CP session level security (Y)es (N)o [N]?
Configure CP name of adjacent node: (Y)es (N)o [N]?
Edit TG Characteristics: (Y)es (N)o [N]?
Edit LLC Characteristics: (Y)es (N)o [N]?
Edit HPR defaults: (Y)es (N)o [N]?
Write this record? [Y]?
The record has been written.
nada207 APPN config>act
nada207 APPN config>exit
nada207 Config>write
Config Save: Using bank B and config number 2
```

Configuración del soporte de Enterprise Extender para HPR sobre IP

```

t 6
Q45 Config>p appn
APPN config>add port
APPN Port
Link Type: (P)PP, (FR)AME RELAY, (E)THERNET, (T)OKEN RING,
(S)DLC, (X)25, (D)LSw, (A)TM, (I)P [ ]? ip
Port name (Max 8 characters) [IP255]?
Enable APPN on this port (Y)es (N)o [Y]?
Port Definition
  Service any node: (Y)es (N)o [Y]?
  Maximum BTU size (768-2048) [768]?
  UDP port number for XID exchange (1024-65535) [11000]?
  UDP port number for low priority traffic (1024-65535) [11004]?
  UDP port number for medium priority traffic (1024-65535) [11003]?
  UDP port number for high priority traffic (1024-65535) [11002]?
  UDP port number for network priority traffic (1024-65535) [11001]?
  IP Network Type: 0 = CAMPUS, 1 = WIDEAREA [0]?
  Local SAP address (04-EC) [4]?
  LDLC Retry Count(1-255) [3]?
  LDLC Timer Period(1-255 seconds) [15]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y ] ?
The record has been written.
***3.3.3.3 is the router's internal IP address
APPN config>add link
APPN Station
Port name for the link station [ ]? ip255
Station name (Max 8 characters) [ ]? tonn
  Activate link automatically (Y)es (N)o [Y]?
  IP address of adjacent node [0.0.0.0]? 3.3.3.3
  Adjacent node type: 0 = APPN network node,
  1 = APPN end node or Unknown node type [0]?
  Allow CP-CP sessions on this link (Y)es (N)o [Y]?
  CP-CP session level security (Y)es (N)o [N]?
  Configure CP name of adjacent node: (Y)es (N)o [N]?
  Remote SAP(04-EC) [4]?
  IP Network Type: 0 = CAMPUS, 1 = WIDEAREA [0]?
  LDLC Retry Count(1-255) [3]?
  LDLC Timer Period(1-255 seconds) [15]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y ] ?
The record has been written.
APPN config>

```

Configuración de redes de conexiones sobre HPR sobre IP

```
t 6
Config>p appn
APPN config>add connection network
Fully-qualified connection network name (netID.CNname) [ ]? supernet.cn1
Port Type: (E)thernet, (T)okenRing, (FR), (A)TM, (FD)DI, (I)P [ ]? ip
    Limited resource timer for HPR (1-2160000 seconds) [180]?
Edit TG Characteristics: (Y)es (N)o [N]?
Write this record? [Y ] ?
The record has been written.
APPN config>add additional port
APPN Connection Networks Port Interface
Fully-qualified connection network name (CPname.CNname) [ ]? supernet.cn1
Port name [ ]? "en000"
Write this record? [Y ] ?
The record has been written.
```

Configuración de un Extended Border Node

```
Spurs APPN config>p app
Spurs APPN config>set node
Enable APPN (Y)es (N)o [N]? y
Network ID (Max 8 characters) [STFDDD3]?
Control point name (Max 8 characters) [SPURS]?
Enable branch extender or extended border node
    (0=Neither, 1=Branch Extender, 2=Border Node)[2]?
Subnet visit count(1-255) [3]?
Cache searches for (0-255) minutes [8]?
Maximum number of searches to cache (0(unlimited)-32765) [0]?
Dynamic routing list updates (0=None, 1=Full, 2=Limited) [1]?
Enable routing list optimization (Y)es (N)o [Y]?
Route addition resistance(0-255) [128]?
XID ID number for subarea connection (5 hex digits) [00000]?
Use enhanced #BATCH COS (Y)es (N)o [Y]?
Use enhanced #BATCHSC COS (Y)es (N)o [Y]?
Use enhanced #INTER COS (Y)es (N)o [Y]?
Use enhanced #INTERSC COS (Y)es (N)o [Y]?
Write this record? [Y ] ?
The record has been written.
Spurs APPN config>act
APPN is not currently active
Spurs APPN config>add rout
Routing list name [ ]? list1
Subnet visit count(1-255) [3]?
Dynamic routing list updates (0=None, 1=Full, 2=Limited) [1]?
Enable routing list optimization (Y)es (N)o [Y]?
Destination LUs found via this list:
    (netID.LUname) [ ] ? net1*
    (netID.LUname) [ ]?
Routing CPs (with optional subnet visit count):
    (netID.CPname ?) [ 3]? net2.router2
    (netID.CPname ?) [ 3]?
Write this record? (Y)es (N)o [Y]?
The record has been written.
```

Uso de APPN

```
Spurs APPN config>add cos
  COS mapping table name []? cos1
  Non-native network (netID.CPname) []? net2.router2
  Non-native network (netID.CPname) []?
  Native and non-native COS name pair [ ]? #inter
  Native and non-native COS name pair [ ]?
Write this record? (Y)es (N)o [Y]?
The record has been written.
```

Uso de TN3270

Esta sección introduce TN3270 y resume la función del servidor de TN3270E, que se implementa en los direccionadores IBM. Incluye los siguientes temas:

- “Visión general”
- “Configuración general del servidor de TN3270E” en la página 94
- “Configuraciones de ejemplo” en la página 109

Visión general

Actualmente muchas empresas consolidan el tráfico de WAN en redes troncales sólo de IP. Las empresas también están simplificando las configuraciones de las estaciones de trabajo e intentando ejecutar sólo la pila de protocolo TCP/IP en el escritorio. Sin embargo, la mayoría de estas empresas todavía necesitan el acceso a sistemas principales de aplicaciones SNA.

TN3270 reúne estos requisitos permitiendo ejecutar IP desde el escritorio a través de la red y conectar con el sistema principal SNA mediante un servidor de TN3270. Los clientes se conectan con el servidor mediante una conexión TCP. El servidor proporciona una función de pasarela para los clientes de TN3270 en sentido directo mediante la correlación de las sesiones de cliente con sesiones de LU-LU dependientes de SNA que el servidor mantiene con el sistema principal SNA. El servidor de TN3270 maneja la conversión entre la corriente de datos de TN3270 y una corriente de datos de SNA 3270.

Para desplegar una solución TN3270, instalará el software de cliente de TN3270 en estaciones de trabajo de escritorio³ y software de servidor de TN3270 en uno de los diversos lugares que se mencionan a continuación. El software de cliente está disponible en IBM y muchos otros fabricantes, y se ejecuta sobre la pila TCP/IP en la estación de trabajo. Un determinado producto cliente proporciona uno de los dos posibles niveles de soporte de estándares:

- Cliente de TN3270 base
Estos clientes cumplen con RFC 1576 (TN3270 Current Practices) y/o RFC 1646 (TN3270 Extensions for LU name and Printer Selection).
- Cliente de TN3270E
Estos clientes cumplen con las RFC 1647 (TN3270 Enhancements) y 2355 (TN3270 Enhancements).

Una implementación de servidor que pueda dar soporte a clientes de TN3270E recibe el nombre de servidor de TN3270E.

³ También puede encontrar pequeños productos de cliente de TN3270 dedicado que representen impresoras.

Ubicación de la función de servidor de TN3270

La función de servidor de TN3270 se puede ubicar en diversos productos y posiciones dentro de una red, incluyendo los siguientes:

- En el sistema principal SNA mismo
IBM y otros fabricantes proporcionan software de servidor de TN3270 que se sitúa sobre la pila TCP/IP y conecta con VTAM dentro del sistema principal.
- En un direccionador o en la red
IBM y otros fabricantes proporcionan la función de servidor de TN3270 en productos de hardware de red. Se pueden colocar dichos productos de forma directamente adyacente al sistema principal SNA o en cualquier posición en la red donde haya conectividad SNA con el sistema principal. Si utiliza direccionadores IBM y el sistema principal ejecuta APPN, puede utilizar la tecnología Enterprise Extender para situar el servidor en cualquier posición donde haya conectividad IP con el sistema principal.
- En un producto de software de la red
IBM y otros fabricantes proporcionan productos de software de servidor de TN3270 que se instalan en servidores de gama media que utilizan sistemas operativos como por ejemplo AIX, OS/2 o Windows NT. Se pueden colocar estos productos en cualquier posición de la red donde haya conectividad SNA con el sistema principal de aplicaciones.

La elección de un producto de servidor de TN3270 y la posición en la red es compleja e implica factores como los siguientes:

- Capacidad del servidor e impacto en el ciclo
- Precio del rendimiento y la capacidad
- Disponibilidad
- Impacto de las anomalías del servidor
- Escalabilidad

Los direccionadores IBM proporcionan una implementación del servidor de TN3270E de alto rendimiento que escala a grandes redes. Mediante la combinación de esta implementación con la característica Network Dispatcher, se puede implementar la redundancia del servidor y el compartimiento de carga en grandes instalaciones TN3270. También se puede ubicar un direccionador IBM en una red SNA o IP fuera del centro de datos y tener las mismas ventajas de escalabilidad, adición de incremento e impacto reducido de las anomalías del servidor.

Función de servidor de TN3270E

Conformidad con la normativa

La implementación de direccionador IBM del servidor de TN3270E da soporte a:

RFC 1576	TN3270 Current Practices
RFC 1646	TN3270 Extensions for LU names and Printers
RFC 1647	TN3270 Enhancements
RFC 2355	TN3270 Enhancements (deja obsoleto a RFC 1647)

Puede manejar tanto clientes base TN3270 como TN3270E al mismo tiempo.

Conectividad con el sistema principal

La vía desde un cliente de 3270 al sistema principal SNA consta de dos partes:

- Una conexión TCP mediante IP desde el cliente al servidor
- Una sesión de LU-LU SNA desde el servidor al sistema principal

La forma de la conexión SNA desde el servidor al sistema principal depende del modo en que el servidor representa las PU y las LU dependientes. Cuando se utiliza un direccionador IBM como servidor de TN3270, se puede configurar de dos formas distintas para establecer enlaces y representar PU y LU ante VTAM:

- Mediante enlaces de subárea SNA

Se configura de este modo cuando no se ejecuta APPN en el sistema principal (aunque el direccionador sigue teniendo capacidad para APPN). Se configura un enlace suelto de capa de DLC con el sistema principal para cada PU (un máximo de 255 LU por cada PU). Varias PU necesitan varios enlaces con el sistema principal paralelos. Las tramas SNA que llegan al direccionador a través de uno de estos enlaces fluyen directamente hacia la PU interna correspondiente.

Los enlaces con el sistema principal de subárea deben ser un único salto de capa de DLC al producto que proporciona la función de frontera de subárea SNA. Normalmente este producto es NCP ejecutándose en un FEP (procesador de componente frontal) o es VTAM mismo en el sistema principal. El enlace de subárea desde el direccionador puede atravesar puentes u otros mecanismos de capa de control de DLC (como por ejemplo convertidores de protocolo o direccionadores DLSw externos). Los direccionadores IBM dan soporte a los siguientes tipos de enlace para la conexión de sistema principal de subárea (donde el tipo de enlace está disponible en un producto direccionador determinado):

- Red en anillo: físico, emulación de LAN ATM o canal LSA
- Ethernet: físico, emulación de LAN ATM o canal LSA
- FDDI: sólo físico
- PVC de frame relay: formatos RFC 1490/2427 puenteados o direccionados
- DLSw (tenga en cuenta que DLSw local puede proporcionar acceso a enlaces SDLC y QLLC de sentido inverso)
- Uso de un enlace petionario de LU dependientes (DLUR) de APPN

Configurará de esta forma cuando ejecute APPN con la función DLUS (Servidor de LU dependientes) en el sistema principal. En el direccionador DLUR, se configurará uno o más DLUS para dar soporte a las PU dependientes internas de TN3270 (y las PU dependientes externas que puedan existir). Un direccionador que ejecute DLUR puede estar conectado directamente al sistema principal de DLUS o puede estar ubicado remotamente a través de diversos enlaces APPN. Sólo es necesario un enlace para realizar el primer o único salto del "conducto" DLUR-DLUS, incluso si se definen varias PU locales (para tener más de 255 LU totales). Las tramas SNA que llegan mediante el conducto DLUR-DLUS fluyen hacia la función DLUR, que las redirecciona hacia la PU interna o externa correcta.

Cuando utilice DLUR, puede direccionar a través de una red APPN mediante el direccionamiento ISR o HPR para llegar al sistema principal. Los direccionadores IBM dan soporte a los siguientes tipos de enlace como enlace APPN de "primer salto" con el sistema principal (donde el tipo de enlace está disponible en un producto direccionador específico):

- Red en anillo: físico, emulación de LAN ATM o canal LSA
- Ethernet: físico, emulación de LAN ATM o canal LSA
- FDDI: sólo físico
- PVC de frame relay: formatos RFC 1490/2427 puenteados o direccionados
- ATM (nativo, no emulación de LAN): sólo HPR
- Canal MPC+: sólo HPR
- PPP
- SDLC: sólo ISR
- X.25: sólo ISR
- DLSw: sólo ISR
- IP (Enterprise Extender): sólo HPR

Tenga en cuenta especialmente que, cuando utilice el direccionamiento HPR y DLUR, puede ubicar un servidor de TN3270E a través de una red IP desde el sistema principal de aplicaciones SNA. Enterprise Extender mantiene la clase de servicio a nivel de sesión y la prioridad de transmisión a través de la red IP.

Si existe una sesión de LU-LU cuando el cliente de TN3270 se desconecta del servidor de TN3270, se enviará una solicitud UNBIND o TERM-SELF al sistema principal para terminar la sesión de LU-LU. El valor por omisión es la limpieza UNBIND. La estación de enlace o PU local debe estar configurada adecuadamente para que fluya TERM-SELF. TERM-SELF debe configurarse si se utiliza un gestor de sesiones (de componente frontal) para llegar a aplicaciones como TSO o CICS.

Soporte de configuración SNA

Desde una consola de operador VTAM o NetView/390, se pueden controlar los enlaces, PU y LU relacionados con TN3270. Para las LU, cuando un cliente de TN3270 se conecta, el direccionador informa acerca de la dirección IP del cliente y del número de puerto TCP a VTAM en los flujos de activación de la sesión (por medio de CV64). Los mandatos de visualización de consola VTAM como por ejemplo "/D NET,ID=(nombre lu),E" tienen la capacidad de mostrar la información de dirección TCP/IP asociada con LU específicas. Esto permite la determinación de problemas para clientes TN3270 desde una consola de operador VTAM.

El soporte VTAM para recibir y mostrar direcciones IP de cliente se encuentra en el CS para el código base OS/390 V2R6. También se han realizado PTF del CS para OS/390 V2R5 (VTAM APAR OW31454, TCP/IP APAR PQ12574).

Además de habilitar este soporte de consola, APPN genera alertas SNA para diversas configuraciones de error y puede reenviar alertas procedentes de otros dispositivos SNA. No hay alertas específicas de la función de servidor de TN3270, pero las alertas que genera el direccionador mismo pueden ser relativas a recursos SNA relacionados con TN3270.

Soporte de detección de condiciones de excepción y MIB de SNMP

Los direccionadores IBM dan soporte a una versión de borrador de Internet de ambas MIB estándar para la función de servidor de TN3270:

- MIB TN3270 Base (ahora RFC 2561)
- MIB TN3270 Response Time (ahora RFC 2562)

El soporte de los direccionadores IBM para estas MIB incluye la posibilidad de:

- Ver la configuración, estado y estadísticas del servidor
- Configurar grupos de clientes para la recogida del tiempo de respuesta
- Ver la correlación de los nombres de LU, como por ejemplo, nombre VTAM, nombre local y dirección IP de cliente
- Ver la correlación de direcciones IP de cliente con nombres de LU VTAM
- Recoger los datos de tiempo de respuesta para los grupos de clientes actuales

Además, la siguiente MIB específica para empresa muestra los motivos por los que los clientes no han podido conectar satisfactoriamente con el servidor de TN3270:

- IBM TN3270 Connection Rejection

Estas MIB relacionadas con TN3270 complementan el amplio soporte de MIB de los direccionadores IBM para recursos SNA y APPN.

Guardado en antememoria de clientes de Host On-Demand de TN3270

Algunos productos direccionadores IBM (actualmente el 2216 y el 2212) dan soporte a una función de "Antememoria de servidor de Web", con lo que pueden situarse delante de un servidor HTTP y descargar el servidor mediante el guardado en antememoria de objetos de Web y sirviéndolos a los clientes que lo soliciten. Entre los objetos que estos direccionadores pueden guardar en antememoria se encuentran applets de Java que proporcionan la función de cliente de TN3270.

El guardado en antememoria de cliente de Host On-Demand (HOD) permite a uno de estos direccionadores o a IBM Network Utility guardar en antememoria applets de función de cliente de TN3270 desde un servidor Web de sistema principal HOD y servirlos a navegadores cliente cuando se efectúe la solicitud. Entonces los navegadores lanzan las applets de emulación de terminal de TN3270. Estas applets conectan con un sistema principal SNA o bien mediante la función de servidor de TN3270 del direccionador o mediante algún otro servidor de TN3270.

El soporte de Host On-Demand viene con la función de servidor de TN3270, pero ambos se configuran independientemente. El direccionador puede guardar en antememoria clientes de HOD pero no configurarse como servidor de TN3270. Asimismo, el direccionador puede ser un servidor de TN3270 sin el guardado en antememoria de HOD habilitado. Las cargas de código del direccionador de Antememoria de servidor de Web que no incluyen la función de servidor de TN3270 (sólo en el 2216 y el 2212) también pueden guardar en antememoria applets de cliente de HOD si se configuran para ello.

Debido a que la función de guardado en antememoria de cliente de HOD es totalmente independiente de la función de servidor, en este capítulo no hay más información sobre este tema. Consulte el capítulo titulado "Configuring and

Monitoring IBM eNetwork Host On-Demand Client Cache” de la publicación *Using and Configuring Features* si desea obtener más información acerca de esta función.

Configuración general del servidor de TN3270E

Esta sección se aporta información general sobre el soporte de la configuración del servidor de TN3270. Si desea ver configuraciones de ejemplo específicas, consulte la sección “Configuraciones de ejemplo” en la página 109.

Carga del código de servidor de TN3270

Dependiendo del tipo de direccionador y del método de configuración, puede que tenga que realizar pasos adicionales para cargar el código de TN3270 y APPN y para tener acceso a las solicitudes de supervisión y configuración de línea de mandatos:

- Instale una carga de código de direccionador que incluya APPN y TN3270. Los protocolos se cargan cuando el direccionador arranca.

Si desea obtener más información sobre el mandato **load add**, consulte el capítulo titulado “The CONFIG Process (CONFIG - Talk 6) and Commands” de la publicación *Guía del usuario de software*.

Configuración de TN3270 bajo el protocolo APPN

En la implementación de los direccionadores IBM de servidor de TN3270, todas las funciones SNA se encuentran empaquetadas dentro del protocolo APPN. Esto significa que, incluso cuando se está configurando la conexión de sistema principal de subárea SNA y el sistema principal SNA no está ejecutando APPN, será necesario utilizar los servicios de consola y configuración del protocolo APPN.

Concretamente:

- Debe pasar por el protocolo APPN en la línea de mandatos y en el Programa de configuración para configurar puertos, enlaces y funciones de servidor de TN3270
- Debe pasar por el protocolo APPN en la línea de mandatos para utilizar los mandatos de supervisión de TN3270
- Debe configurar APPN a nivel del nodo

Al configurar el soporte de subárea SNA, en realidad el direccionador todavía funciona como nodo de red APPN, pero sólo en enlaces con otros nodos APPN. Si los únicos puertos y enlaces que se configuran son los destinados a la conexión de sistema principal de subárea SNA, la función APPN no se ejecutará por sí misma.

Dirección IP del servidor

Para habilitar la función de servidor de TN3270, será necesario configurar una dirección IP a la que los clientes de TN3270 se conectarán. La implementación de TN3270 de los direccionadores IBM da soporte sólo a una única dirección IP de servidor (pero a varios puertos TCP de destino). La dirección que se configure para TN3270 debe coincidir con una de las siguientes direcciones que se configuren para IP, de lo contrario TN3270 no se inicializará.

- Una dirección de interfaz

Se puede asignar un número ilimitado de direcciones a una interfaz. Puede tratarse de una interfaz física o bien de una interfaz virtual "de bucle de retorno". Las direcciones de interfaz física están activas sólo cuando la interfaz asociada está activa, mientras que las direcciones de interfaz de bucle de retorno están siempre activas.

- La dirección interna

Es una única dirección que representa todo el direccionador y que está activa independientemente del estado de cualquier interfaz específica.

Cuando se elige la dirección IP para la función de TN3270, debe tener en cuenta que los usuarios administrativos también deben poder establecer sesiones normales de Telnet para activar consolas de direccionador remotas. El puerto de destino por omisión tanto para Telnet como para TN3270 es el mismo (23), por lo que a menos que desee que uno o que los demás conjuntos de usuarios utilicen un puerto de destino que no sea el valor por omisión, debe reservar distintas direcciones IP para los usuarios de TN3270 y Telnet.

Si utiliza el código de direccionador V3.4 o superior, el procedimiento que se recomienda es definir una interfaz de bucle de retorno y utilizar una de las direcciones IP de dicha interfaz como dirección IP del servidor de TN3270. Si utiliza el código de direccionador anterior a V3.4, será necesario optar entre utilizar una dirección de interfaz física para TN3270 y dejar la dirección interna para Telnet o viceversa. Algo importante a tener en cuenta en esta elección es si se tienen varios servidores de TN3270 paralelos, cada uno de los cuales necesita la misma dirección de servidor y distintas direcciones Telnet para su mantenimiento.

Puertos TCP del servidor

Al configurar la dirección IP del servidor, se especifica también un número de puerto TCP de destino al que los clientes de TN3270 se conectarán. Se debe proporcionar como mínimo un número de puerto como parte de la configuración general del servidor (TN3270E config> set command, Configuration Program TN3270E Server/General panel). Opcionalmente, se pueden configurar puertos TCP adicionales en los que el servidor de TN3270 "escuchará" (TN3270E config> add port command, Configuration Program TN3270E Server/Ports panel).

Es posible que desee configurar más de un puerto TCP de servidor por los motivos siguientes:

- Separe los clientes "E" de los "no E"

El protocolo TN3270 necesita un servidor capacitado para E para iniciar ciertas negociaciones con los clientes. Algunos antiguos clientes que no son E presentan una anomalía en lugar de simplemente hacer caso omiso de estas negociaciones. Se puede configurar el direccionador de modo que trate a los clientes que se conecten con un determinado puerto de destino como no E, por lo que no les enviará la solicitud en cuestión. Entonces se configurarán los clientes no E de modo que se conecten a dicho puerto.

- Correlacione los clientes con los recursos SNA mediante un número de puerto
- Muchos clientes no pueden solicitar un recurso SNA por el nombre, pero todos ellos se conectan con un puerto TCP de destino. Al configurar un puerto de destino, se asocia una agrupación de LU con dicho puerto (hay una agrupación global por omisión si no se especifica ninguna en concreto). A los clientes que

se conecten con este puerto y no especifiquen ningún nombre de LU, se les asignará una LU de esta agrupación.

- Inhabilite la correlación de direcciones IP para algunos clientes

Si ha habilitado globalmente la correlación de direcciones IP de cliente con nombres de LU o de agrupación de LU, el direccionador elige la LU mediante las normas de correlación de direcciones IP en lugar de utilizar el puerto para la asociación de agrupación de LU. Puede optar por tener un conjunto de clientes que queden exentos de esta correlación (tenga en cuenta que a los clientes que no coinciden con las correlaciones configuradas se les rechaza la conexión). Puede configurar un puerto de destino de modo que, cuando un cliente conecte con ese puerto, se ignorará la correlación de direcciones IP. Cuando seleccione esta opción, para elegir la LU se utilizará la agrupación de LU asociada con dicho puerto.

- Correlacione los clientes con los recursos SNA mediante la correlación de direcciones IP específica del puerto

Si ha habilitado globalmente la correlación de direcciones IP de cliente con nombres de LU o de agrupación de LU, puede que desee que se apliquen distintas normas de correlación de IP a los distintos conjuntos de clientes. Cuando configure una entrada de tabla de correlación de IP, puede especificar un número de puerto TCP de destino (el valor por omisión es "all ports" (todos los puertos)). Si lo hace, sólo se comprobarán los clientes que se conecten con dicho número de puerto para ver si coinciden con una entrada de correlación.

Definición de las PU

Siempre deben definirse las PU dependientes en el direccionador, para que contengan las LU que el direccionador asocia con las conexiones TCP de clientes de TN3270 entrantes. Cada PU que se define debe tener una definición de PU correspondiente en VTAM.

Si utiliza DLUR para la conexión de sistema principal, cada una de las PU internas que se definen parecen tener un enlace lógico "incluido" con la función DLUR. Este enlace lógico está siempre activo cuando APPN y TN3270 están activos. Al mismo tiempo puede que DLUR esté sirviendo a otras PU dependientes externas al direccionador.

Es necesario definir sólo el número de PU que sean necesarias para contener las LU. Cada PU puede tener 255 LU. Si se define más de una PU local, se pueden distinguir unas de otras especificando distintos ID de nodo local. Para configurar una PU local para DLUR a través de la línea de mandatos, utilice el mandato **add local-pu**. Desde el programa de configuración, seleccione Local PUs (PU locales) bajo el protocolo TN3270E Server (Servidor de TN3270E) en la ventana de navegación.

Si utiliza enlaces de subárea para la conexión de sistema principal, cada enlace está ligado a una PU interna asociada. El direccionador crea esta PU interna automáticamente cuando se configura un enlace de subárea; no se configuran PU internas de forma explícita tal como se hace con DLUR. En enlace asociado con cada PU es un enlace real externo que puede ir hacia arriba o hacia abajo. Algunos usuarios distribuyen las LU de una única agrupación a través de varias PU de subárea, de modo que si un enlace es anómalo podrá haber otro disponible para dar servicio a los intentos de reconexión por parte de clientes.

Para configurar un enlace de subárea a través de la línea de mandatos, utilice el mandato add link. Responda yes a la pregunta "Solicit SSCP session?" (¿Solicitar sesión SSCP?) y no a la pregunta "Does link support APPN function?" (¿El enlace da soporte a la función APPN?). Desde el programa de configuración, seleccione Interfaces bajo el protocolo APPN en la ventana de navegación y luego pulse en la cabecera de columna Link stations (Estaciones de enlace). Si configura más de un enlace de subárea bajo el mismo puerto físico, debe habilitar dicho puerto de modo que soporte varias PU. Se pueden distinguir las PU por el ID de nodo local y también por la información de direccionamiento local como por ejemplo la dirección SAP.

Definición de las LU

Cuando un cliente de TN3270 está plenamente conectado, la conexión TCP se empareja con una representación de LU SNA en el servidor. VTAM también tiene una representación para la misma LU. Cada una de estas representaciones de LU tiene un nombre, y es posible pero no necesario que el nombre de LU del servidor coincida con el nombre de LU de VTAM. Debido a que una configuración de TN3270 típica comprende cientos de LU que se deberán satisfacer como clientes potenciales, se han desarrollado varios esquemas para facilitar la tarea de configurar las LU y hacer posible que los nombres del servidor y de VTAM coincidan.

La implementación de los direccionadores IBM de servidor de TN3270 actualmente da soporte a los siguientes métodos de definición de LU. Consulte las secciones siguientes si desea obtener una descripción detallada de cada método. Todos estos métodos están disponibles independientemente de si la conexión de enlace del sistema principal es DLUR o subárea.

- Estático en el direccionador, estático en el sistema principal

Con este método, se configuran las LU en el direccionador individualmente por nombre o en grupos utilizando gérmes de nombre. Se pueden definir las LU correspondientes en VTAM a mano utilizando nombres de LU iguales o distintos. Las direcciones NAU de LU y el ID de PU son lo que relaciona las LU del direccionador con las LU de VTAM.

- Estático en el direccionador, dinámico en el sistema principal (DDDLU - Definición dinámica de LU dependientes)

Con este método también se configuran LU en el direccionador individualmente por nombre o en grupos utilizando gérmes de nombre. En VTAM, se pueden codificar definiciones de LU modelo y asociarlas con las PU dependientes definidas en el direccionador. Cuando un cliente de TN3270 conecta con el direccionador, el direccionador selecciona una LU y envía la información configurada sobre dicha LU a VTAM (tanto el nombre como la dirección NAU). El paso del nombre de LU del direccionador de esta forma recibe el nombre de "empujar el nombre". VTAM crea la definición de LU de forma dinámica, utilizando su propio germen de nombre o el nombre de LU que el direccionador ha "pasado".

Cuando un cliente de TN3270 desconecta, el direccionador envía una notificación de este suceso. Niveles posteriores de VTAM tienen la capacidad de destruir la LU dinámica. Las versiones anteriores no destruyen la LU, sino que simplemente la desactivan colgando la utilización por parte de otro cliente. La creación y supresión dinámicas hacen posible que la misma LU nombrada esté servida por cualquiera de diversos servidores de TN3270 paralelos con carga equilibrada.

- Dinámico en el direccionador, estático en el sistema principal (HIDLU - LU dinámicas iniciadas por el sistema principal)

Con este método, no es necesario configurar las LU en el direccionador. Simplemente se configura en base a que una PU da soporte a las LU dinámicas iniciadas por el sistema principal. En VTAM, se definen las PU y las LU a mano de la forma normal. Al activar las LU en VTAM, las ACTLU hacen que el direccionador cree dinámicamente las LU correspondientes usando el nombre de LU de VTAM. Las LU dinámicas se tratan como LU explícitas o se ubican en agrupaciones de LU implícitas en base a si se configura un nombre de agrupación para la PU con capacidad para HIDLU.

Se puede seleccionar cualquiera de estos métodos de definición de LU, en base al tamaño de la configuración de red, nivel de direccionador y código VTAM, requisitos de denominación de LU y requisitos de equilibrio de carga del servidor. Se puede combinar HIDLU con los otros métodos configurando algunas LU del direccionador y permitiendo que el resto se creen dinámicamente, incluso dentro de la misma PU.

LU configuradas

Es necesario configurar las LU del direccionador a menos que esté utilizando LU dinámicas iniciadas por el sistema principal. Se pueden configurar LU individuales o grupos de LU. Normalmente se configuran LU individuales cuando se desea especificar completamente el nombre de LU y fijarlo en una dirección NAU específica. Se configuran grupos de LU cuando se tiene un gran número de LU parecidas por definir y se desea que el direccionador genere los nombres de LU.

Para configurar una LU individual desde la línea de mandatos, use el mandato **add lu**. Deberá especificar el nombre de PU (o enlace de subárea) de la LU y el nombre, tipo y dirección NAU de la LU. Para configurar una LU individual desde el Programa de configuración, seleccione LUs bajo el protocolo TN3270E Server en la ventana de navegación y luego pulse la cabecera de columna LUs.

Para configurar un grupo de LU desde la línea de mandatos, use el mandato **add implicit-pool**. Este mandato define un grupo de LU bajo una única PU y las coloca en una agrupación. Se puede usar este mandato varias veces para colocar distintos grupos de LU en la misma agrupación, como por ejemplo las LU de distintas PU.

Cada vez que añada un grupo, especificará el nombre de PU, el nombre de agrupación e información del tipo de LU. En lugar de una única dirección NAU, especificará un rango de direcciones o el número de LU que desee añadir. En el momento de la inicialización, el direccionador fija las direcciones NAU para las LU individuales configuradas y luego asigna las direcciones restantes del rango o el número de direcciones a las LU del grupo.

En lugar de un único nombre de LU, para un grupo es necesario especificar una máscara de nombre de LU. Cuando el direccionador se inicializa, asigna los nombres de LU añadiendo como sufijo esta máscara a la dirección NAU de la LU en decimal (no añadiéndole ceros iniciales). Por ejemplo, una máscara "@LU1A" puede resultar en los nombres de LU @LU1A1, @LU1A2, etc.

Si especifica un rango de direcciones NAU, el direccionador genera nombres añadiendo la dirección NAU empezando por la parte inferior del rango que va hacia

la parte superior, tal como se acaba de mostrar con @LU1A. Si especifica el número de LU en lugar de un rango de direcciones NAU, el direccionador genera nombres empezando por NAU 2, incrementando hasta 255 y acabando en 1. Por ejemplo, una máscara de @LU2A para 10 LU generaría los nombres @LU2A2, @LU2A3, ..., @LU2A11. El código de servidor empieza con un 2 para la consistencia de migración con releases de código anteriores que no soportaban el valor NAU 1. Para ver los nombres exactos que el direccionador genera para las LU bajo una PU específica, use el mandato de Talk 5 TN3270 **list pu nombre**.

Para configurar un grupo de LU desde el Programa de configuración, en primer lugar debe nombrar la agrupación de destino mediante la selección de Pools bajo el protocolo TN3270E Server en la ventana de navegación. Luego seleccione LUs en la ventana de navegación y pulse la cabecera de columna Implicit Pool.

Definición dinámica de LU dependientes (DDDLU)

Tal como se indica en Definición de las LU, se puede utilizar DDDLU para evitar definiciones duplicadas de LU tanto en VTAM como en el direccionador. DDDLU le permite configurar LU sólo en un lugar: el direccionador. En VTAM, sólo es necesario definir una o más PU, dependiendo del número de LU que sean necesarias. La implementación de DDDLU también elimina el esfuerzo del mantenimiento y las definiciones de VTAM para requisitos de definición de LU futuros.

Creación de LU en VTAM

Cuando un cliente TN3270E solicita una conexión utilizando una de las LU definidas en el direccionador, éste envía un mandato Reply PSID NMVT a VTAM en la sesión SSCP-PU. En este mandato, el direccionador envía la información siguiente:

- Dirección NAU local de la LU
- Nombre de direccionador para la LU
- Indicador de encendido y apagado
- Tipo y número de modelo del dispositivo
- Demás información opcional dependiente de los dispositivos

Al recibir este NMVT, a partir de la definición de la PU VTAM ve que no hay definición para la LU en cuestión. Entonces VTAM usa la definición de PU y la información del NMVT para seleccionar una sentencia de LU modelo y crear una definición de LU.

El nombre que VTAM elige para la LU dinámica es conducido por una rutina de salida para la Selección de definiciones para LU dependientes (SDDL). Si se utiliza la rutina de salida de usuario estándar proporcionada por IBM, VTAM construye un nombre utilizando el valor LUSEED de la sentencia de PU, con la dirección NAU añadida como sufijo. También debe codificar el operando LUGROUP para especificar un nodo mayor modelo. Estas operaciones se describen en *VTAM Network Implementation Guide*, SC31-8370, bajo la sección titulada "Defining Dependent LUs Dynamically".

Si desea que VTAM use el nombre de LU que el direccionador envía en el mandato Reply PSID NMVT, debe sustituir la salida de usuario SDDL estándar por una que esté disponible en las páginas Web para bajarse el soporte de direccionadores IBM. Esta rutina desatiende el operando LUSEED y simplemente utiliza el nombre que se ha empujado desde el direccionador. Para bajarse esta

rutina desde las páginas Web 2216, por ejemplo vaya a <http://www.networking.ibm.com/support/downloads/2216>, seleccione el enlace a "APPN/TN3270 Files" y seleccione el paquete de salida de usuario. El paquete es común a todos los direccionadores IBM.

Supresión de LU desde VTAM

Cuando un cliente TN3270 se desconecta del direccionador, envía a VTAM otra Reply PSID NMVT indicando que el dispositivo se ha apagado. Entonces VTAM puede eliminar la LU creada dinámicamente. Esto libera espacio y hace que el nombre vuelva a estar disponible para ser utilizado.

El soporte VTAM para la supresión de LU dinámica en la desconexión de clientes está en el código base del CS para OS/390 V2R6 y hay PTF del CS para OS/390 V1R3 y posterior con el APAR OW29773.

LU dinámicas y Network Dispatcher

Network Dispatcher de IBM (ND) puede proporcionar una función de equilibrio de carga TCP cuando se instala entre clientes y dos o más servidores de TN3270. La versión de direccionador IBM de ND y TN3270 Server funcionan juntos, de forma que ND envía nuevas conexiones de cliente al servidor de TN3270 menos ocupado. Anteriormente, al utilizar ND para equilibrar la carga entre servidores de TN3270 que iban al mismo VTAM, no se podían tener LU que necesitaran un nombre de LU de VTAM fijo. Esto es debido a que ND podía direccionar la conexión TCP de cliente a cualquiera de los servidores, pero no se podían tener nombres de LU duplicados activos en VTAM al mismo tiempo.

Con el empuje y la supresión del nombre de LU, se puede configurar el nombre de LU deseado y todos los servidores de TN3270 potenciales. Cuando el cliente se conecta, el servidor que ND selecciona envía el nombre a VTAM para la creación dinámica. Cuando el cliente se desconecta, VTAM puede suprimirlo. Así vuelve a estar disponible para ser creado de nuevo a través del servidor de TN3270 que ND seleccione la próxima vez que el cliente se conecte.

Detalles adicionales

El ejemplo siguiente muestra una definición de PU de VTAM para DDDL. Tenga en cuenta que las diversas LU estáticas necesitan nombres de LU específicos e impresoras 3270 en puertos específicos, también se definen bajo el mismo nodo principal conmutado.

Ejemplo:

```
DDDPV VBUILD TYPE=SWNET
DDPU  PU ADDR=02,           x
      IDBLK=077,           x
      IDNUM=22160,         x
      PUTYPE=2,            x
      USSTAB=US327X,       x
      LUGROUP=GROUP1,      x
      LUSEED=DDLU###,      x
      DLOGMOD=D4C32XX3
SALE01 LU  LOCADDR=98,      x 1
      DLOGMOD=D4C32XX3,    x
      LOGAPPL=CICSA
SALEPRT LU  LOCADDR=99,    x 2
      LOGMODE=SAL3287,     x
      LOGAPPL=CICSA
```

1 En esta definición de ejemplo se ha solicitado que la LU 'SALE01' esté en LOCADDR=98 debido a requisitos específicos. Por lo tanto, esta LU específica se define bajo esta 'DDDP' para cumplir los requisitos.

2 En esta definición, la impresora también debe estar en una dirección específica. Esto ocurre especialmente para algunas aplicaciones SNA (por ejemplo, CICS). La aplicación para el departamento de ventas necesita una impresora en la dirección 99, con LOGMODE=SAL3287, y debe estar conectada con la aplicación CICS cuando se active.

Para los usuarios que desean escribir su propia rutina de salida o modificar una de las rutinas de salida SDDL de VTAM, el direccionador envía información de LU en la respuesta PSID NMVT del modo siguiente:

- En SV10, el subcampo 11 contiene uno de los valores de tipo de modelo y dispositivo listados en Tabla 3.
- En SV86, el subcampo 00 contiene IBMTN3270LUNAME para indicar que se está empujando un nombre de LU
- En SV86, el subcampo 10 contiene el nombre de LU real en EBCDIC

A continuación se encuentra un ejemplo de estos subvectores:

```
191000 161103130012F3F2F7F0F0F0F2      (3270 device - mod 2)
1D86   1100C9C2D4E3D5F3F2F7F0D3E4D5C1D4C5 (IBMTN3270LUNAME)
        0A10C1C1C1C1C2C2C2C2             (LU name is AAAABBBB)
```

Tabla 3. Valores de tipo de dispositivo/modelo

Dispositivo/modelo	Vector NMVT
Pantalla 3270 mod 2	3270002
Pantalla 3270 mod 3	3270003
Pantalla 3270 mod 4	3270004
Pantalla 3270 mod 5	3270005
Impresora 3270	3270P
Impresora SCS	SCSP

Definición dinámica iniciada por un sistema principal de LU dependientes (HIDLU)

Tal como se resume en “Definición de las LU” en la página 97, HIDLU elimina la carga de configurar LU en el direccionador haciendo que el direccionador cree LU dinámicamente a medida que se activan desde VTAM. Esto es esencialmente lo contrario de DDDL, donde el usuario configura las LU en el direccionador y las crea dinámicamente en VTAM. HIDLU permite la definición de las LU sólo en VTAM. En el direccionador se define sólo una PU o tantas como sean necesarias, pero no las LU para dichas PU.

Cuando VTAM activa la PU y sus LU, se llevan los nombres de LU de VTAM al direccionador en los mandatos ACTLU en Control Vector 0E. Las LU definidas de este modo tienen el mismo nombre tanto en VTAM como en el direccionador.

Para configurar HIDLU en el direccionador, también debe definir las PU dependientes locales del direccionador para DLUR o para enlaces de subárea, tal como

se describe en “Definición de las PU” en la página 96. Al configurar la PU de DLUR o el enlace de subárea, simplemente debe indicar que las LU dinámicas iniciadas por el sistema principal deben estar permitidas para esta PU. También se debe indicar si estas LU dinámicas deben colocarse en una agrupación o no, especificando opcionalmente un nombre de agrupación. Si no especifica un nombre de agrupación, serán tratadas sólo como LU de estación de trabajo. Si especifica un nombre de agrupación, puede indicar si se trata de LU de estación de trabajo o de impresora. Todas las LU de HIDLU agrupadas bajo una PU específica deben estar en la misma agrupación y tener el mismo tipo. Puede utilizar el mismo nombre de agrupación para varias PU si desea más de 255 LU en la agrupación o si desea que la agrupación abarque varios enlaces de subárea.

Si coloca HIDLU en una agrupación, no será necesario configurar clientes para solicitar de modo explícito una LU específica. Los clientes pueden solicitar una LU por nombre de agrupación, utilizando una dirección IP para la correlación de agrupaciones o utilizando un puerto TCP para la correlación de agrupaciones. También puede combinar LU explícitas con LU agrupadas por HIDLU configurando una LU individual bajo una PU que esté configurada con una agrupación iniciada por un sistema principal. Cuando la ACTLU llega para la LU individual configurada, el direccionador no crea una LU dinámica.

Para configurar HIDLU en VTAM, es necesario definir las LU dependientes en el nodo principal y especificar INCLUD0E=YES en la sentencia de PU. La palabra clave INCLUD0E es soportada por VTAM V4R4 con los APAR OW31805 y OW31436. Para las conexiones de subáreas remotas a través de NCP, se necesita V7R6 para el soporte de la palabra clave INCLUD0E.

Si el sistema principal es un DLUS y la PU está recibiendo servicio de un DLUR en otro nodo, es posible que el CV0E de la solicitud ACTLU no se reenvíe a la PU desde el DLUR. En tal caso, las LU no se crearán dinámicamente. Una vez creadas dinámicamente, las LU sólo se pueden eliminar suprimiéndolas manualmente mediante la configuración o volviendo a arrancar el sistema. Si se cambian los nombres de LU en el archivo de nodo principal del sistema principal después de crear dinámicamente las LU, los nombres locales del direccionador no cambiarán.

Correlación de clientes con LU

Cuando un cliente de TN3270 se conecta con un servidor, el servidor debe seleccionar una LU para asociarla con dicho cliente o denegar la conexión. Hay diversas formas de configurar los clientes y el servidor para que controlen qué LU se seleccionarán y a qué clientes se denegará la conexión. La implementación de los direccionadores IBM de servidor de TN3270 da soporte a los siguientes métodos:

- El cliente puede solicitar un nombre de LU individual
- El cliente puede solicitar un nombre de agrupación de LU
- Se puede configurar el direccionador para que correlacione direcciones IP con LU individuales configuradas o con nombres de agrupaciones de LU.
- Se puede configurar el direccionador para que asocie números de puerto TCP de destino con nombres de agrupaciones de LU configurados

Las secciones siguientes describen los conceptos de fondo, cómo configurar cada uno de estos métodos y cómo funcionan.

Conceptos

Agrupaciones de LU y LU individuales: Tal como se describe anteriormente en “LU configuradas” en la página 98, se pueden configurar LU individuales o grupos de LU del direccionador. Además, las LU dinámicas iniciadas por un sistema principal se pueden tratar individualmente o en grupos. Una agrupación de LU es simplemente un grupo de LU nombrado. Por ejemplo, puede poner el nombre MYPOOLA a una agrupación.

Las LU de una agrupación pueden venir de una o distintas PU. Exceptuando las LU dinámicas iniciadas por el sistema principal, las LU que se encuentran bajo una PU pueden colocarse en varias agrupaciones. Las LU que se colocan en una agrupación específica normalmente tienen definiciones VTAM parecidas y también características como la utilización del mismo USSMSG10. La utilización de agrupaciones es el método principal para agrupar LU parecidas y en último lugar se correlacionaría un conjunto de usuarios del extremo del cliente de TN3270 con agrupaciones específicas.

La agrupación global por omisión: Hay siempre como mínimo una agrupación definida para TN3270E Server, a la que se hace referencia como Agrupación global por omisión. Se nombra esta agrupación al configurar inicialmente TN3270E Server y, por omisión, tiene el nombre PUBLIC. Sea cual sea el nombre que se ponga a la agrupación por omisión, se puede hacer referencia a dicho nombre en otras partes de la configuración del servidor utilizando una serie de caracteres especial <DEFLT >. Eso le permitirá cambiar más adelante el nombre de agrupación en sólo un lugar sin tener que cambiar todas las referencias al mismo. Sin embargo, tenga en cuenta que la serie <DEFLT> tiene un significado especial cuando se utiliza en una entrada de la tabla de correlaciones de dirección IP, por lo que debe intentar entender este significado al definir tales correlaciones.

Puede que no necesite tener una agrupación por omisión, pero existirá de todas formas. Sin embargo, no es necesario poner ninguna LU en esta agrupación.

LU explícitas e implícitas: Las LU del servidor de TN3270 pueden dividirse en dos categorías, en base a cómo se permite a los clientes acceder a las mismas. Las LU implícitas son siempre miembros de una agrupación y los clientes pueden acceder a las mismas por su nombre individual o por cualquiera de los métodos que utilizan los nombres de agrupación. Se configuran LU implícitas añadiendo un grupo de éstas a una agrupación o añadiendo LU individuales a una agrupación. Las LU explícitas nunca son miembros de una agrupación (incluso de la agrupación global por omisión), por lo que pueden acceder a las mismas sólo clientes que solicitan su nombre individual o por correlaciones de dirección IP con dicho nombre. La función de servidor nunca asignará una LU explícita a un cliente que solicite o esté correlacionado con un nombre de agrupación.

Clientes que solicitan nombres de LU

Las implementaciones de cliente que dan soporte a los RFC 1646 ó 2355 pueden solicitar un nombre de recurso cuando se conectan a un servidor de TN3270. En el servidor del direccionador IBM, este nombre se trata como un nombre de LU individual o como nombre de agrupación. En la configuración de cliente, puede hacerse referencia al mismo como nombre de LU a pesar de que el mismo nombre está configurado en el direccionador como nombre de agrupación.

Si el método de definición de LU utilizado implica distintos nombres de LU en el direccionador y VTAM, el nombre que el cliente pasará debe coincidir con el nombre de LU del direccionador y no con el nombre de LU en VTAM.

Ante la ausencia de dirección IP y correlación de puerto TCP, el servidor intenta satisfacer la solicitud de cliente del modo siguiente:

- Si el cliente solicita un nombre de LU individual y está disponible, se asignará la LU. Si no está disponible, el servidor denegará la conexión.
- Si el cliente solicita un nombre de agrupación válido y una LU de dicha agrupación está disponible, se asignará la LU. Si no hay ninguna LU disponible, el servidor denegará la conexión.
- Si el nombre solicitado no es válido, el servidor denegará la conexión.

Consulte las secciones siguientes para ver lo que sucede cuando un cliente, un nombre y uno de los métodos de correlación también son aplicables.

Correlación de direcciones IP de cliente con LU/agrupaciones

Se puede configurar la función de servidor de TN3270 del direccionador para que correlacione direcciones IP de cliente con nombres de LU individuales o nombres de agrupaciones de LU. Puede que desee hacerlo si los clientes no tienen la capacidad de solicitar nombres de recursos o si no desea configurar los clientes individualmente. También puede que desee utilizar esta función como mecanismo de seguridad, para denegar conexiones con clientes que no estén en la lista de accesos de correlaciones IP.

Para configurar esta función de correlación, primero debe habilitarla globalmente como parte de la configuración global del servidor de TN3270. Si desea que los clientes que conecten con ciertos puertos TCP del servidor estén exentos de la correlación de direcciones IP, puede inhabilitar esta función puerto por puerto cuando se configuren los puertos. Entonces creará una tabla de entradas de correlación de direcciones IP, cada una de las cuales correlaciona un conjunto de direcciones IP con una única LU o nombre de agrupación. Por omisión, una entrada determinada es aplicable a todos los puertos TCP del servidor, pero se puede especificar que debe utilizarse una entrada sólo para las conexiones efectuadas con un cierto puerto TCP de destino. Esto permitirá que clientes de distintas redes IP utilicen el mismo conjunto de números de puerto pero se correlacionen con distintas agrupaciones de LU en base tanto a la red como al número de puerto del servidor de destino.

Los campos clave en cada entrada de correlación son: una dirección IP, una máscara de dirección IP y una LU o nombre de agrupación de LU. La máscara de dirección IP indica los bits de la dirección IP configurada que deben compararse con los bits correspondientes de la dirección IP de origen del cliente entrante. Esto permitirá correlacionar o bien clientes sueltos o subredes enteras.

Por ejemplo, si la entrada de correlación está definida como:

```
IP Address: 1.2.3.4
Subnet Mask: 255.255.255.255
Pool or LU: MYLU
```

Si un cliente de TN3270 se conecta utilizando la dirección IP 1.2.3.4, TN3270E Server asignará MYLU a este cliente. Aquí correlacionamos una dirección IP indivi-

dual con una LU individual. También se pueden correlacionar clientes específicos con una agrupación.

Si la entrada de correlación está definida como:

IP Address: 1.2.3.4
Subnet Mask: 255.255.255.0
Pool or LU: YOURPOOL

Si un cliente de TN3270 se conecta utilizando una dirección IP de 1.2.3.1, 1.2.3.2 ó 1.2.3.3, ..., etc., el TN3270E Server asignará al cliente una LU de YOURPOOL. Debido a que la máscara de subred es 255.255.255.0, todos los clientes de esta subred coincidirán con esta entrada de correlación. Las máscaras que no son 255.255.255.255 deben correlacionarse con una agrupación y no con una LU individual.

Suponga que define ambas entradas de correlación anteriores. Tenga en cuenta que el cliente 1.2.3.4 coincidiría con ambas entradas de correlación. TN3270E Server siempre utilizará en primer lugar la coincidencia más específica. En este ejemplo, el cliente se correlacionaría con la LU llamada MYLU.

Suponga de nuevo que ambas entradas de correlación anteriores están definidas y que el cliente 1.2.3.4 se conecta. TN3270 elegirá la entrada de correlación más específica e intentará conectar con la LU llamada MYLU. Sin embargo, por alguna razón el servidor no puede establecer satisfactoriamente la sesión con MYLU; podría ser que MYLU ya esté en uso o puede que no haya sido activada por VTAM. Después de intentar sin éxito la conexión con MYLU, el servidor normalmente explora la tabla de correlación de direcciones IP para ver si hay otra coincidencia menos específica para este cliente. En nuestro ejemplo hay otra coincidencia y TN3270E Server conectaría el cliente con una LU de YOURPOOL.

Hay casos donde es posible que no desee que el direccionador utilice una coincidencia menos específica después de que otra más específica presente alguna anomalía. Para controlar este comportamiento, puede configurar opcionalmente una entrada como "final LU mapping connection attempt" (intento de conexión de correlación de LU final). Si se establece este distintivo de yes/no (sí/no), la función de servidor no busca coincidencias menos específicas después de una coincidencia anómala en esta entrada.

El servidor de TN3270 efectúa las comprobaciones siguientes cuando un cliente se conecta con el direccionador y no pasa una solicitud de nombre específica:

1. Si la correlación está habilitada globalmente, ¿la correlación está habilitada en el puerto de destino? Si no lo está, las solicitudes entrantes se tratan sin utilizar la correlación de direcciones IP.
2. Si es así, intente la coincidencia entre la dirección IP de cliente entrante y las entradas de correlación en este orden:
 - a. para entradas para el puerto de destino específico, la dirección IP más específica en primer lugar
 - b. para entradas para todos los puertos de destino, dirección IP más específica en primer lugar
3. Si hay alguna coincidencia, intente emparejar la conexión con la LU indicada o una LU de la agrupación indicada, respetando el tipo de LU (estación de trabajo o impresora) solicitado por el cliente

4. Si hay un problema y esta no es la entrada de correlación "final", vuelva a intentarlo con coincidencias menos específicas. Antes de denegar la conexión, continúe hasta que se agoten todas las coincidencias o se realice satisfactoriamente la conexión.
5. Si no hay ninguna coincidencia, deniegue la conexión

Cuando un cliente se conecta y solicita un nombre específico, la lógica de coincidencia es distinta. Para conectar satisfactoriamente, debe existir una entrada de correlación cuya dirección IP y máscara coincidan con el cliente y cuyo nombre de recurso sea exactamente igual que el nombre que el cliente ha pasado. Si el cliente solicita un nombre de LU individual, dicho nombre debe estar en la tabla de correlaciones, no sólo el nombre de una agrupación que contenga dicha LU. El servidor no busca en la tabla de correlaciones la coincidencia entre la dirección IP y la máscara más específica. Si la conexión con la LU/agrupación no puede satisfacerse con el nombre solicitado, el servidor no vuelve a explorar la tabla de correlaciones para encontrar otras entradas coincidentes.

Se puede utilizar la correlación de la lista de mandatos Talk 5 de TN3270 para ver el orden en el que se buscarán las entradas de correlación. Se puede poner una dirección IP específica como parámetro de este mandato, para ver sólo las entradas de correlación que sean aplicables a dicha dirección IP.

Aquí se encuentran diversas consideraciones adicionales importantes para construir entradas de correlación de direcciones IP:

- Si tiene varias entradas que son igualmente específicas, primero se utilizarán las que se hayan definido más recientemente.
- Si la agrupación global por omisión tiene el nombre PUBLIC y se configura una entrada de correlación con el nombre PUBLIC, el servidor conectará a los clientes entrantes con las LU de dicha agrupación. Sin embargo, si configura una entrada de correlación con el nombre <DEFLT>, el servidor no conectará a los clientes con la agrupación PUBLIC. En su lugar, pasará a las normas de asociación de puertos TCP y conectará el cliente con la agrupación asociada con el puerto del servidor de destino con el que el cliente se ha conectado.
- La tabla de correlaciones de direcciones IP es creada inicialmente por el servidor TN3270E con una entrada por omisión que contiene la dirección IP 0.0.0.0, la máscara de subred 0.0.0.0 y el nombre de agrupación <DEFLT>. Esta entrada coincidirá con todas las direcciones de cliente entrantes. Tal como se ha mencionado anteriormente, ocasionará que el servidor correlacione clientes con las LU de la agrupación asociada con el puerto o puertos TCP de destino. Si prefiere no tener esta entrada por omisión en la tabla de correlaciones de nombres de LU, puede crear una entrada parecida por encima de la misma correlacionándola con una agrupación nombrada e indicar que la suya es la última que se buscará. Si la agrupación nombrada es la agrupación global por omisión, puede optar por no configurar ninguna LU de dicha agrupación.
- Los nombres de LU y de agrupación que se configuren en entradas de correlación IP deben configurarse en el direccionador para que puedan pasar a ser activos. Por ejemplo, no se pueden configurar nombres de LU dinámicas individuales iniciadas por el sistema principal en entradas de correlación IP, ya que dichos nombres no son conocidos para el direccionador en el momento de la inicialización. Sin embargo, se pueden configurar nombres de agrupación HIDLU, ya que éstos se configuran en el direccionador.

- Para LU de estación de trabajo individuales con impresoras asociadas, tanto las LU de estación de trabajo como las de impresora deben tener una entrada de tabla de correlaciones IP con la misma dirección IP de cliente.
- La especificación de un número de puerto en una entrada de tabla de correlaciones de direcciones IP no hace que el servidor de TN3270 defina el puerto y escuche en el mismo las conexiones de cliente. Será necesario configurar el puerto explícitamente (utilizando **add port**) para que una referencia al mismo en esta tabla tenga algún significado.

Asociación del puerto TCP del servidor con una agrupación

Se puede configurar la función de servidor de TN3270 del direccionador para correlacionar conexiones de cliente entrantes con agrupaciones de LU en base al número de puerto TCP al que los clientes se están conectando. Puede que desee hacerlo si los clientes no tienen la capacidad de solicitar nombres de recursos o si no desea configurar los clientes individualmente. También es posible que esté migrando una red ya existente donde los clientes ya se conectan con distintos números de puerto TCP en base a las necesidades de aplicaciones.

Para configurar la asociación de un puerto TCP con una agrupación, debe especificarse un número de agrupación con el puerto al configurarlo (consulte la sección “Puertos TCP del servidor” en la página 95). Los clientes obviamente tienen que conectarse a través de uno de los puertos definidos y la función del servidor asigna una LU en base a la agrupación que se ha asociado con el puerto. Si no se especifica un número de agrupación para un puerto o si se da el valor especial <DEFLT>, la agrupación global por omisión se asocia con dicho puerto. Se trata de la misma agrupación que se asocia con el puerto del servidor globalmente definido cuando se configura por primera vez el servidor de TN3270.

Si un cliente se conecta y no pasa un nombre de recurso, la función de servidor de TN3270 asigna una LU de la agrupación asociada con el puerto de destino. Si no hay LU disponibles, se rechaza la conexión.

Si un cliente se conecta y pasa un nombre de LU o de agrupación de LU específico, son aplicables las normas siguientes:

- Si el puerto está asociado exactamente con el mismo nombre de LU o de agrupación que el que ha pasado el cliente, éste se conectará con la LU o una LU de la agrupación (si hay una disponible).
- Si el puerto está definido con un nombre de agrupación nulo o con el nombre <DEFLT>, se conectará al cliente con la LU específica o con una LU de la agrupación que el cliente ha pasado, siempre que dicho nombre exacto de LU o de agrupación esté configurado en algún lugar del servidor de TN3270E. Una LU individual puede ser explícita o implícita. El tipo de LU o agrupación (estación de trabajo, impresora SCS o impresora 3270) debe coincidir con la solicitud. Si se trata de un nombre de LU, no importa la agrupación en la que la LU está agrupada, si la hay.
- Si no se da ninguna de las dos condiciones anteriores o si la LU o las LU especificadas no están disponibles, se rechaza la conexión.

En la descripción anterior se asume que la correlación IP está inhabilitada. Si la correlación de direcciones IP está habilitada, por omisión la función de correlación de direcciones IP se aplica a todos los puertos y prevalecerá sobre la correlación de puerto TCP con una agrupación. Se puede cambiar este comportamiento por

omisión inhabilitando la correlación de direcciones IP en un puerto TCP, tal como se ha descrito anteriormente. Tenga en cuenta también el caso especial en el que una entrada de correlación de direcciones IP con la agrupación <DEFLT> puede ocasionar la asignación de LU desde la agrupación asociada con el puerto TCP.

Combinación de la correlación de dirección IP y puerto

Es posible utilizar una combinación de la correlación de direcciones IP y de la asociación de puerto TCP con una agrupación. A continuación se encuentra un ejemplo de cómo un usuario ha combinado estos métodos para satisfacer sus necesidades de correlación.

- El usuario tenía la correlación de direcciones IP habilitada y había definido entradas de correlación para que correlacionasen subredes IP de cliente específicas con agrupaciones específicas.
- Los mismos clientes del usuario final se dieron cuenta de la necesidad de conectar ocasionalmente con un grupo de LU que presentaba una pantalla de conexión USSMSG10 distinta.
- Ya que se trataba del mismo conjunto de clientes, utilizarían las mismas direcciones IP, por lo que la adición de entradas de correlación adicionales a la tabla de correlación de direcciones IP no resolvería sus necesidades.
- El usuario definió una nueva agrupación de LU, definió un nuevo puerto y lo asoció con la nueva agrupación. Además, definió este nuevo puerto de modo que no utilizase la tabla de correlación de direcciones IP, lo que resultaría en la utilización de las agrupaciones originales.
- Entonces los clientes se configuraron en las estaciones de trabajo del usuario final de forma que se conectasen con el nuevo puerto.

Equilibrio de carga entre varias PU

Es frecuente definir una gran agrupación de LU que residen en varias PU. Cualquier agrupación con más de 255 LU debe incluir más de una PU. La diseminación de las LU de una agrupación entre varias PU puede disminuir el número de clientes afectados por cualquier anomalía en un enlace o PU. El modo que tiene el servidor de asignar LU entre estas diversas PU también determina el número de clientes que se ven afectados por una anomalía en un enlace o en una PU. Por ejemplo, si el servidor ha asignado todas las LU a una PU antes de asignar alguna a la segunda PU, una posible anomalía en la primera puede afectar a incluso 255 clientes innecesariamente.

La implementación TN3270 de los direccionadores IBM generalmente efectúa una asignación firmada en rueda de las LU de distintas PU de una agrupación. Con todas las demás cosas iguales, asignará la LU1 de PU1, la LU1 de PU2, etc. Al mismo tiempo, el algoritmo de asignación favorece a las PU que están activas actualmente (evitando el retardo de un intento de activación) y favorece a las LU que proporcionan una coincidencia exacta con el tipo de modelo solicitado por el cliente.

Las normas para la selección de LU son las siguientes:

- Una coincidencia exacta en base al tipo de modelo siempre se devuelve si se encuentra en una PU activa.

- Si no se puede encontrar una coincidencia exacta en una PU activa, se devolverá una LU aceptable de una PU activa antes que una coincidencia exacta de una PU inactiva.
- Para tratarse de una coincidencia “aceptable”, el tipo de LU (estación de trabajo, impresora SCS o impresora 3270) debe coincidir con lo que el cliente está solicitando. El tipo de modelo para una LU de estación de trabajo debe dar el mismo tamaño de pantalla o uno menor que el que el cliente ha solicitado. Por ejemplo, si un cliente ha solicitado un modelo 4, una LU de modelo 4 sería una coincidencia exacta y las LU de modelo 3 ó 2 serían coincidencias aceptables.

En base a si se encuentra una coincidencia exacta o aceptable, las PU se mueven a una lista para proporcionar una asignación general firmada en rueda y al mismo tiempo impedir que se busque primero en las PU menos deseables.

Configuraciones de ejemplo

Esta sección contiene ejemplos de configuraciones de línea de mandatos del direccionador y de VTAM para entornos básicos de servidor de TN3270. Si desea ver entornos más avanzados e información de configuración del programa, consulte la sección “Otras configuraciones de ejemplo” en la página 114.

Configuración de TN3270 mediante DLUR

Si está usando DLUR para comunicarse con el sistema principal, las PU locales usadas por el servidor de TN3270E deberán configurarse en el sistema principal como PU internas de DLUR. El código siguiente es un ejemplo de configuración de VTAM del sistema principal:

```

PUJOE7  PU  ADDR=12,
          IDBLK=077, IDNUM=EEEE7, 1
          MAXPATH=8,
          ISTATUS=ACTIVE,
          MODETAB=LMT3270,
          USSTAB=STFTSNA2,
          ANS=CONT,
          MAXDATA=521,
          IRETRY=YES,
          MAXOUT=7,
          DLOGMOD=G22NNE,
          NETID=STFNET,
          PASSLIM=5,
          PUTYPE=2
JCPATH7  PATH  PID=1,
          DLURNAME=VLNN01,
          DLCADDR=(1,C,INTPU),
          DLCADDR=(2,X,07711111)
JC7LU2   LU   LOCADDR=2
JC7LU3   LU   LOCADDR=3
JC7LU4   LU   LOCADDR=4
JC7LU5   LU   LOCADDR=5
JC7LU6   LU   LOCADDR=6

```

Nota: **1** 07711111 representa el bloque de ID/número de ID de la PU local. La parte 077 de este valor no se puede configurar en el direccionador.

El ejemplo siguiente muestra cómo configurar el direccionador de modo que utilice una conexión DLUR de sentido inverso para TN3270, utilizando la línea de mandatos.

```

APPN config>
APPN config>set node
Enable APPN (Y)es (N)o [Y]?
Network ID (Max 8 characters) [STFNET]?
Control point name (Max 8 characters) [VLNN2]?
Enable branch extender (Y)es (N)o [N]?
Route addition resistance(0-255) [128]?
XID ID number for subarea connection (5 hex digits) [00000]?
Use enhanced #BATCH COS (Y)es (N)o [Y]?
Use enhanced #BATCHSC COS (Y)es (N)o [Y]?
Use enhanced #INTER COS (Y)es (N)o [Y]?
Use enhanced #INTERSC COS (Y)es (N)o [Y]?
Write this record? [Y ] ?
    The record has been written.
APPN config>
APPN config>
APPN config>set dlur
Enable DLUR (Y)es (N)o [Y]?
Fully-qualified CP name of primary DLUS [STFNET.MVS8]?
Fully-qualified CP name of backup DLUS []?
Perform retries to restore disrupted pipe [Y]?
Delay before initiating retries(0-2756000 seconds) [120]?
Perform short retries to restore disrupted pipe [Y]?
Short retry timer(0-2756000 seconds)[120]?
Short retry count(0-65535) [5]?
Perform long retry to restore disrupted pipe [Y]?
Long retry timer(0-2756000 seconds) [300]?
Write this record? [Y ] ?
    The record has been written.
APPN config>
APPN config>tn3270e
TN3270E config>set
TN3270E Server Parameters
Enable TN3270E Server (Y/N) [Y]?
TN3270E Server IP Address[4.3.2.1]?
Port Number[23]?
Enable Client IP Address to LU Name Mapping (Y/N) [N]
Default Pool Name[PUBLIC]?
NetDisp Advisor Port Number[10008]?
    Keepalive type:
        0 = none,
        1 = Timing Mark,
        2 = NOP[2]?
Frequency ( 1 - 65535 seconds)[60]?
Automatic Logoff (Y/N)[N]?
Write this record? [Y ] ?
    The record has been written.

```

```

APPN config>tn3270
TN3270E config>exit
APPN config>
APPN config>add loc
Local PU information
Station name (Max 8 characters)[]? link1
Fully-qualified CP name of primary DLUS[STFNET.MVS8] ?
Fully-qualified CP name of a backup DLUS[]?
Local Node ID (5 hex digits)[11111]?
Autoactivate (y/n)[Y]?
Write this record? [Y ] ?
  The record has been written.
TN3270E config>add im
TN3270E Server Implicit definitions
Pool name (Max 8 characters)[<DEFLT>]?
Station name (Max 8 characters)[]? link1
LU Name Mask (Max 5 characters) [@01LU]?
  LU Type      ( 1 - 3270 mod 2 display
                2 - 3270 mod 3 display
                3 - 3270 mod 4 display
                4 - 3270 mod 5 display) [1]?
Specify LU Address Range(s) (y/n) [n]
  Number of Implicit LUs in Pool(1-255) [50]?
Write this record? [Y ] ?
  The record has been written.
TN3270E config>
TN3270E config>add lu
TN3270E Server LU Definitions
LU name(Max 8 characters) []? printer1
  NAU Address (1-255) [0] 2
Station name (Max 8 characters)[]? link1
  Class:
    1 = Explicit Workstation,
    2 = Implicit Workstation,
    3 = Explicit Printer,
    4 = Implicit Printer[3]?
  LU Type ( 5 - 3270 printer
            6 - SCS printer) [5]?
Write this record[Y]?
  The record has been written.
TN3270E config>
TN3270E config>list all
TN3270E Server Definitions
TN3270E enabled: YES
TN3270E IP Address: 4.3.2.1
TN3270E Port Number: 23
Keepalive type: NOP          Frequency: 60
Automatic Logoff: N         Timeout: 30
  Enable IP Precedence: N
Link Station: link1
  Local Node ID: 11111
  Auto activate : YES
  Implicit Pool Informationø
    Number of LUs: 50
    LU Mask: @01LU
  LU Name   NAU addr   Class           Assoc LU Name   Assoc   NAU addr
-----
printer1   2           Explicit Printer

```

```

TN3270E config>exit
APPN Config>exit

```

```
Config>
Config>p ip
Internet protocol user configuration
IP config>li all
Interface addresses
IP addresses for each interface:
  intf 0  9.1.1.20      255.0.0.0      Local wire broadcast, fill 1
  intf 1
interface
  intf 2
interface
Internal IP address: 4.3.2.1

Routing

Protocols
BOOTP forwarding: disabled
IP Time-to-live: 64
Source Routing: enabled
Echo Reply: enabled
TFTP Server: enabled
Directed broadcasts: enabled
ARP subnet routing: disabled
ARP network routing: disabled
Per-packet-multipath: disabled
OSPF: disabled
BGP: disabled
RIP: disabled

IP config>
*
```

Configuración de TN3270E usando una conexión de subárea

El ejemplo siguiente muestra cómo configurar el direccionador de modo que utilice una conexión de sistema principal de sentido inverso de subárea SNA (no APPN) para TN3270, utilizando la línea de mandatos. En este ejemplo, el direccionador aparece ante VTAM como varias PU en sentido directo.

```
Config>p appn
APPN config>set node
Enable APPN (Y)es (N)o [Y]?
Network ID (Max 8 characters) [STFNET]?
Control point name (Max 8 characters) [VLNN2]?
Enable branch extender (Y)es (N)o [N]?
Route addition resistance(0-255) [128]?
XID ID number for subarea connection (5 hex digits) [00000]?
Use enhanced #BATCH COS (Y)es (N)o [Y]?
Use enhanced #BATCHSC COS (Y)es (N)o [Y]?
Use enhanced #INTER COS (Y)es (N)o [Y]?
Use enhanced #INTERSC COS (Y)es (N)o [Y]?
Write this record? [Y ] ?
  The record has been written.
APPN config>
```



```

APPN config>add port
  APPN Port
  Link Type: (P)PP, (FR)AME RELAY, (E)THERNET, (T)OKEN RING,
  (S)DLC, (X)25, (FD)DI, (D)LSw, (A)TM, (I)P [ ]?fr
  Interface number(Default 0):[0]? 2
  Port name (Max 8 characters) [F00002]?
  Enable APPN on this port (Y)es (N)o [Y ] ?
  Port Definition
  Support multiple subarea (Y)es (N)o [N]? y
  All active port names will be of the form <port name sap>
    Service any node: (Y)es (N)o[Y]?
  High performance routing: (Y)es (N)o [Y]? n
  Maximum BTU size (768-8136) [2048]?
    Percent of link stations reserved for incoming calls (0-100)[0]?
    Percent of link stations reserved for outgoing calls (0-100)[0]?
    Local SAP address (04-EC) [4]?
    Support bridged formatted frames: (Y)es (N)o [N]?
  Edit TG Characteristics: (Y)es (N)o [N ] ?
  Edit LLC Characteristics: (Y)es (N)o [N]?
  Edit HPR defaults: (Y)es (N)o [N]?
  Write this record? [Y ] ?
  The record has been written.
APPN config>add link
  APPN Station
  Port name for the link station [ ]#? f00002
  Station name (Max 8 characters) [ ]? suba1
    Activate link automatically (Y)es (N)o[Y]?
  DLCI number for link (16-1007) [16]? 23
    Adjacent node type: 0 = APPN network node,
    1 = APPN end node or Unknown node type,
    2 = LEN end node [0]?
  Solicit SSCP Session: (Y)es (N)o [N]? y
  Local Node ID (5 hex digits) [00000]? 12345
  Local SAP address (04-EC) [4]? c
  Allow CP-CP sessions on this link (Y)es (N)o [Y]? n
    Configure CP name of adjacent node: (Y)es (N)o[N]?
  Edit TG Characteristics: (Y)es (N)o [N ] ?
  Edit LLC Characteristics: (Y)es (N)o [N]?
  Edit HPR defaults: (Y)es (N)o [N]?
  Write this record? [Y ] ?
  The record has been written.
APPN config>act
APPN config>
APPN config>tn3270e
TN3270E config>set
TN3270E Server Parameters
  Enable TN3270E Server (Y/N) [Y]?
  TN3270E Server IP Address[4.3.2.1]?
  Port Number[23]?
  Enable Client IP Address to LU Name Mapping (Y/N) [N]
  Default Pool Name[PUBLIC]?
  NetDisp Advisor Port Number[10008]?
    Keepalive type:
    0 = none,
    1 = Timing Mark,
    2 = NOP[2]?
  Frequency ( 1 - 65535 seconds)[60]?
  Automatic Logoff (Y/N)[N]?
  Write this record? [Y ] ?
  The record has been written.
TN3270E config>exit

```

```

APPN config>
Write this record? [Y ] ?
  The record has been written.
TN3270E config>add im
TN3270E Server Implicit definitions
Pool name (Max 8 characters) [<DEFLT>]?
Station name (Max 8 characters) []? suba1
LU Name Mask (Max 5 characters) [@01LU]?
Specify LU Address Range(s) (y/n) [N]
  Number of Implicit LUs in Pool(1-255) [50]?
Write this record? [Y ] ?
  The record has been written.
TN3270E config>
TN3270E config>add lu
TN3270E Server LU Definitions
LU name(Max 8 characters) []? printer1
  NAU Address (1-255) [2]
Station name (Max 8 characters) []? suba1
Class:
  1 = Explicit Workstation,
  2 = Implicit Workstation,
  3 = Explicit Printer,
4 = Implicit Printer[3]?
  LU Type ( 5 - 3270 printer
    6 - SCS printer) [5]?
Write this record[Y]?
  The record has been written.
TN3270E config>
TN3270E config>list all
TN3270E Server Definitions
TN3270E enabled: YES
TN3270E IP Address: 4.3.2.1
TN3270E Port Number: 23
Keepalive type: NOP          Frequency: 60
Automatic Logoff: N          Timeout: 30
  Enable IP Precedence: N
Link Station: suba1
  Local Node ID: 12345
  Auto activate : YES
  Implicit Pool Informationø
    Number of LUs: 50
    LU Mask: @01LU
  LU Name  NAU addr  Class          Assoc LU Name  Assoc  NAU addr
-----
printer1  2          Explicit Printer

```

```

TN3270E config>exit
APPN Config>exit

```

```

APPN config>act

```

Otras configuraciones de ejemplo

El modelo TN1 del producto Network Utility se ha diseñado para utilizarse como servidor de TN3270 y se suministra con información de configuración de TN3270 que puede ser útil para los usuarios de 2216, 2212 y 2210. Esta información está disponible tanto en publicaciones del producto como en archivos de configuración binarios de ejemplo en la Web.

La publicación *Network Utility: Installation, Getting Started, and User's Guide*, GA27-4167-02, documenta la configuración del direccionador (normalmente tanto la

línea de mandatos como el programa de configuración) y las configuraciones de VTAM de ejemplo para las siguientes configuraciones de red:

- Conexión de sistema principal de subárea a través de una red en anillo con un NCP (igual que para una pasarela de canal u OSA)
- Servidores de TN3270 de subárea paralelos con equilibrio de carga por parte de dos direccionadores Network Dispatcher
- Conexión DLUR de sistema principal a través de red en anillo con un nodo de red
- Conexión DLUR de sistema principal a través de Enterprise Extender con una pasarela direccionador IBM
- Definición dinámica de LU dependientes (DDDLU)
- Definición dinámica de LU iniciadas por el sistema principal (HIDLU)
- Antememoria de cliente de Host On-Demand (HOD)
- Conexión de sistema principal de subárea por encima de DLSw
- Conexión de sistema principal de subárea por encima de un canal por medio de un bucle de retorno LSA

Algunas de las configuraciones anteriores se complementan en la Web con archivos de configuración binarios tanto en formato de direccionador como en formato de programa de configuración. Use el navegador para llegar a ellos del modo siguiente:

1. Abra la página de bajada de Network Utility en:
<http://www.networking.ibm.com/support/downloads/networkutility>
2. Siga el enlace con los archivos de "Configuration Program" (programa de configuración)
3. Busque el release del código que utiliza (el contenido del archivo ya ha sido actualizado para cada release)
4. Abra el paquete llamado "Example Configuration Files" (Archivos de configuración de ejemplo)

Configuración y supervisión de APPN

Este capítulo describe los mandatos de supervisión y configuración de APPN. Está formado por las secciones siguientes:

- “Resumen de los mandatos de configuración de APPN”
- “Información detallada sobre los mandatos de configuración de APPN” en la página 119
- “Soporte de reconfiguración dinámica de APPN” en la página 283

Acceso al proceso de configuración de APPN

Siga el procedimiento siguiente para acceder al proceso de *configuración* de APPN.

1. En el indicador *, entre **talk 6**. Se visualizará el indicador Config>. (Si no se visualiza, pulse de nuevo **Intro**).
2. Entre **protocol appn**. Aparecerá el indicador APPN Config>.
3. Entre un mandato de configuración de APPN.

Resumen de los mandatos de configuración de APPN

Tabla 4 (Página 1 de 3). Resumen de los mandatos de configuración de APPN

Mandato	Función	Consulte página:
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte la sección “Cómo obtener ayuda” en la página xxix.	
Enable/Disable	Activa/desactiva: APPN Dependent LU Requestor Port <i>nombre del puerto</i>	119
Set	Establece los elementos siguientes: Node Traces HPR DLUR Management Tuning	119 136 125 128 152 131
Add	Añade o actualiza los parámetros siguientes: Port <i>nombre del puerto</i>	155

Mandatos de configuración de APPN (Talk 6)

Tabla 4 (Página 2 de 3). Resumen de los mandatos de configuración de APPN		
Mandato	Función	Consulte página:
	Link-station <i>nombre de la estación de enlace</i>	176
	LU-Name <i>Nombre LU</i>	197
	Connection-network <i>nombre de la red de conexiones</i>	198
	Additional-port-to-connection-network	207
	Mode	206
	Focal_point	208
	local-pu	208
	Routing_list	211
	COS_mapping_table	215
Delete	Suprime los elementos siguientes: <ul style="list-style-type: none"> • Port <i>nombre del puerto</i> • Link-station <i>nombre de la estación de enlace</i> • LU-Name <i>Nombre LU</i> • Connection-network <i>nombre de la red de conexiones</i> • Connection networks port interface (CN PORTIF) <i>nombre CN</i> • Mode <i>nombre modalidad</i> • Focal_point • local-pu • Routing_list • COS_mapping_table 	217
List	Lista los elementos siguientes de la memoria de configuración: <ul style="list-style-type: none"> • All • Node • Traces • Management • HPR • DLUR • Port <i>nombre del puerto</i> • Link-station <i>nombre del enlace</i> • LU-Name <i>Nombre LU</i> • Mode <i>nombre modalidad</i> • Connection-network <i>nombre de la red de conexiones</i> • Focal_point • Routing_list • COS_mapping_table 	217
Activate_new_config	Lee la configuración en memoria de configuración no volátil.	217
TN3270	Da acceso al indicador de mandatos TN320E config>	218

Tabla 4 (Página 3 de 3). Resumen de los mandatos de configuración de APPN		
Mandato	Función	Consulte página:
Exit	Le devuelve al nivel de mandatos anterior. Consulte la sección “Cómo salir de un entorno de nivel inferior” en la página xxix.	

Nota: APPN responderá a un mandato **reset** dinámico en el nivel de interfaz.

Información detallada sobre los mandatos de configuración de APPN

Enable/Disable

Use el mandato **enable/disable** para habilitar (o inhabilitar):

Sintaxis:

```
enable          appn
[o disable]   dlur
                port nombre del puerto
```

Set

Use el mandato **set** para establecer:

Sintaxis:

```
set            node
```

Se le solicitará que entre los valores para los parámetros siguientes. El rango del parámetro se mostrará entre paréntesis (). El valor por omisión del parámetro se mostrará entre corchetes [].

Tabla 5 (Página 1 de 6). Lista de parámetros de configuración - Direccionamiento de APPN	
Información de los parámetros	
Parámetro	Enable APPN
Valores válidos	Yes (Sí), No
Valor por omisión	Yes
Descripción	<p>Este parámetro habilita o inhabilita al direccionador como nodo de red APPN.</p> <p>Este parámetro habilita la posibilidad de direccionamiento de HPR y APPN para este nodo de red, posibilidad que consiste en definir el ID de red y el nombre del CP de este nodo. No obstante, APPN debe habilitarse en los puertos determinados donde desee dar soporte al direccionamiento APPN. Además, el soporte para HPR debe habilitarse en los puertos APPN deseados y debe tener soporte de las estaciones de enlace concretas de dichos puertos.</p> <p>Nota: HPR sólo tiene soporte en puertos DLC directos de LAN, Frame Relay y PPP.</p>

<i>Tabla 5 (Página 2 de 6). Lista de parámetros de configuración - Direccionamiento de APPN</i>	
Información de los parámetros	
<p>Parámetro Network ID (obligatorio)</p> <p>Valores válidos Una serie de 1 a 8 caracteres:</p> <ul style="list-style-type: none"> • Primer carácter: De la A a la Z • Del segundo al octavo carácter: De la A a la Z, de 0 a 9 <p>Nota: Se sigue dando soporte a un identificador de una red existente, en la que el nodo de red del direccionador va a entrar como miembro, y que usa los caracteres especiales @, \$ y # del juego de caracteres A; no obstante, dichos caracteres no deben usarse en los ID de red nuevos.</p> <p>Valor por omisión Ninguno</p> <p>Descripción Este parámetro especifica el nombre de la red APPN a la que pertenece este nodo de red. El ID de red debe ser el mismo para todos los nodos de la red APPN. Los nodos finales APPN y los nodos finales LEN conectados pueden tener ID de red diferentes.</p>	
<p>Parámetro Control point name (obligatorio)</p> <p>Valores válidos Una serie de 1 a 8 caracteres:</p> <ul style="list-style-type: none"> • Primer carácter: De la A a la Z • Del segundo al octavo carácter: De la A a la Z, de 0 a 9 <p>Nota: Sigue dándose soporte a nombres de CP ya existentes que adquiera este nodo y que en su nombre tengan los caracteres especiales @, \$ y # del juego de caracteres A; no obstante, no deberán usarse estos caracteres en los nombres de CP nuevos.</p> <p>Valor por omisión Ninguno</p> <p>Descripción Este parámetro especifica el nombre del CP para este nodo de red APPN. El CP es responsable de la gestión del nodo de red APPN y de sus recursos. El nombre del CP es el nombre lógico del nodo de red APPN de la red. Este nombre debe ser único dentro de la red APPN y debe identificarse mediante el parámetro Network ID.</p>	
<p>Parámetro Enable branch extender or border node</p> <p>Valores válidos 0 (no habilitar ninguno)</p> <p>1 (habilitar branch extender)</p> <p>2 (habilitar el nodo de frontera)</p> <p>Valor por omisión 0</p> <p>Descripción Este parámetro especifica si la función de Branch Extender, la de nodo de frontera o ninguna de las dos se habilitará en el nodo. Si habilita alguna de estas dos funciones, se harán las preguntas adicionales apropiadas.</p>	

Tabla 5 (Página 3 de 6). Lista de parámetros de configuración - Direccionamiento de APPN	
Información de los parámetros	
Parámetro Valores válidos Valor por omisión Descripción	Enable Branch Awareness Support 0 (Completo), 1 (Parcial), 2 (Ninguno) 0 (Completo) Este parámetro especifica si desea limitar el flujo de información de topología acerca de la topología de Branch Extender. <i>Completo</i> significa que el nodo difundirá todos los TG de Branch Extender en la red cuando se sepan. <i>Parcial</i> significa que el nodo no difundirá la topología de Branch Extender local, pero almacenará y difundirá la topología de Branch Extender no local. <i>Ninguno</i> significa que el nodo no difundirá la topología de Branch Extender local y que pasará por alto la topología de Branch Extender que reciba procedente de la red y el nodo no almacenará ni difundirá topología de Branch Extender no local.
Parámetro Valores válidos Valor por omisión Descripción	Permit search for unregistered LUs Yes o No No Este parámetro especifica si pueden efectuarse búsquedas de LU en este nodo (cuando actúa como nodo final) si las LU no se registraron en el servidor de nodos de red de Branch Extender. Si especificó <i>yes</i> , se pueden buscar LU en este nodo. Nota: Esta pregunta sólo se efectúa si el parámetro Enable Branch Extender or Border Node está en <i>branch extender</i> .
Parámetro Valores válidos Valor por omisión Descripción	Subnet visit count De 1 a 255 3 Especifica el valor por omisión del nivel de nodo para el número máximo de subredes que puede atravesar una sesión de varias subredes. El valor por omisión puede alterarse temporalmente como parte de la configuración de una lista de direccionamientos, enlaces o puertos. Nota: Esta es la primera de una serie de preguntas que se hacen sólo si se ha habilitado el nodo de frontera.
Parámetro Valores válidos Valor por omisión Descripción	Cache searches for (0-255) minutes De 0 a 255 8 Especifica cuántos minutos retiene el BN información en la antememoria de búsqueda de varias subredes una vez finalizada ésta.
Parámetro Valores válidos Valor por omisión Descripción	Maximum number of searches in cache De 0 a 32765 (0=ilimitado) 0 Especifica el número máximo de entradas en la antememoria de búsqueda de varias redes. Una vez alcanzado el límite, se descartarán las entradas más antiguas. Nota: El mecanismo primario de supresión de estas entradas es el valor del tiempo de búsqueda en antememoria especificado en cache searches for (0–255) minutes .

<p>Tabla 5 (Página 4 de 6). Lista de parámetros de configuración - Direccionamiento de APPN</p>	
<p>Información de los parámetros</p>	
<p>Parámetro</p>	<p>Dynamic routing list updates</p>
<p>Valores válidos</p>	<p>0 (ninguna) - No se añaden entradas dinámicas.</p> <p>1 (completa) - Se añaden todos los nodos de frontera nativos, todos los nodos de red y de frontera no nativos adyacentes y los nodos que saben LU de destino con nombres similares.</p> <p>2 (limitada) - Se añaden todos los nodos de frontera nativos, todos los nodos de red y los de frontera no nativos adyacentes con el mismo IDRED y los nodos que saben LU de destino con nombres similares.</p>
<p>Valor por omisión</p>	<p>2</p>
<p>Descripción</p>	<p>Indica el grado, si hay alguno, hasta el que un BN puede añadir a los datos de la lista configurada de direccionamientos, datos topológicos aprendidos por el código operativo. Estos datos adicionales no se guardan en la SRAM.</p>
<p>Parámetro</p>	<p>Enable routing list optimization</p>
<p>Valores válidos</p>	<p>Yes o No</p>
<p>Valor por omisión</p>	<p>Yes</p>
<p>Descripción</p>	<p>Indica si un BN puede volver a ordenar o no la copia temporal de una lista de direccionamientos de subred del código operativo, para que las entradas que tengan más posibilidades de éxito se encuentren primero.</p>
<p>Parámetro</p>	<p>Load balance across parallel inter-subnet boundaries</p>
<p>Valores válidos</p>	<p>Yes o No</p>
<p>Valor por omisión</p>	<p>No</p>
<p>Descripción</p>	<p>Este parámetro especifica si el direccionador debe intentar equilibrar el número de sesiones entre dos o más puntos de salida paralelos entre subredes cuando funciona como EBN. La configuración relevante tiene dos o más direccionadores IBM que sirven como puntos de salida EBN en una subred con el mismo número en la otra subred. Cada direccionador tiene un TG entre subredes hacia un direccionador distinto en la otra subred, que forman dos o más enlaces paralelos. (Tenga en cuenta que no se trata de TG paralelos entre cualquier par de direccionadores.)</p> <p>Para configurar el equilibrio de carga de sesión entre los puntos de salida paralelos:</p> <ol style="list-style-type: none"> 1. Establezca este parámetro en <i>yes</i>. 2. Configure listas de direccionamiento (consulte la página 210) en cada direccionador EBN, de modo que las sesiones para nombres de LU de destino distintos tengan EBN de salida preferibles distintos. También se configurará el límite entre subredes preferible y se podrán establecer recorridos de seguridad. 3. Configure las listas de direccionamiento con dynamic routing list updates establecido en <i>none</i> y Enable routing list optimization establecido en <i>no</i>. <p>Nota: Esta es la última de una serie de preguntas que se hacen sólo si se ha activado el nodo de frontera.</p>

<i>Tabla 5 (Página 5 de 6). Lista de parámetros de configuración - Direccionamiento de APPN</i>	
Información de los parámetros	
Parámetro	Route addition resistance
Valores válidos	De 0 a 255
Valor por omisión	128
Descripción	Este parámetro indica el deseo de direccionar a través de este nodo. Se usa en el cálculo de la ruta basado en la clase de servicio. Los valores inferiores indican mayores niveles de deseabilidad.
Parámetro	XID number for subarea connection (consulte las notas de la tabla)
Valores válidos	Una serie de 5 dígitos hexadecimales
Valor por omisión	X'00000'
Descripción	<p>Este parámetro especifica un número de ID único (identificador) para el nodo de red. El número de XID se combina con un número de bloque de ID (que identifica un producto específico) para formar una identificación de nodo XID. Las identificaciones de nodo se intercambian entre nodos adyacentes cuando éstos están estableciendo una conexión. El nodo de red del direccionador añade automáticamente un número de bloque de ID a este parámetro durante el intercambio de XID para crear una identificación de nodo XID.</p> <p>El número de ID que asigne a este nodo debe ser único dentro del nodo APPN identificado por el parámetro Network ID. Póngase en contacto con el administrador de red para verificar que el número de ID sea único.</p>
Nota:	<p>Por lo general, las identificaciones de nodo se intercambian entre nodos T2.1 durante el establecimiento de la sesión de CP-CP. Si el nodo de red está comunicando con el producto IBM Virtual Telecommunications Access Method (VTAM) a través del nodo LEN T2.1 y éste tiene definido para él un nombre de CP, el parámetro de número XID no es necesario. Si el nodo LEN adyacente no es T2.1 o no tiene un nombre de CP definido explícitamente, el parámetro de número de XID deberá especificarse para establecer una conexión con el nodo LEN. Las versiones de VTAM anteriores a la versión 3 release 2 no permiten definir nombres de CP para los nodos LEN.</p>
Parámetro	Use enhanced BATCH COS
Valores válidos	Yes o No
Valor por omisión	Yes
Descripción	<p>Este parámetro especifica si deben utilizarse tablas de COS mejoradas. Estas tablas asignan pesos razonables a TG de ATM basándose en el coste, velocidad y retardo. Para ATM, el orden de preferencia es:</p> <ul style="list-style-type: none"> • Campus Best Effort (SVC o PVC)/Reserved PVC (WAN o Campus) • Campus Reserved SVC • WAN Best Effort (SVC o PVC) • WAN Reserved SVC

<i>Tabla 5 (Página 6 de 6). Lista de parámetros de configuración - Direccionamiento de APPN</i>	
Información de los parámetros	
Parámetro	Use enhanced BATCHSC COS
Valores válidos	Yes o No
Valor por omisión	Yes
Descripción	<p>Este parámetro especifica si deben utilizarse tablas de COS mejoradas. Estas tablas asignan pesos razonables a TG de ATM basándose en el coste, velocidad y retardo. Para ATM, el orden de preferencia es:</p> <ul style="list-style-type: none"> • Campus Best Effort (SVC o PVC)/Reserved PVC (WAN o Campus) • Campus Reserved SVC • WAN Best Effort (SVC o PVC) • WAN Reserved SVC
Parámetro	Use enhanced INTER COS
Valores válidos	Yes o No
Valor por omisión	Yes
Descripción	<p>Este parámetro especifica si deben utilizarse tablas de COS mejoradas. Estas tablas asignan pesos razonables a TG de ATM basándose en el coste, velocidad y retardo. Para ATM, el orden de preferencia es:</p> <ul style="list-style-type: none"> • Campus Reserved (SVC o PVC) • Campus Best Effort (SVC o PVC)/WAN reserved PVC • WAN Reserved SVC • WAN Best Effort (SVC o PVC)
Parámetro	Use enhanced INTERSC COS
Valores válidos	Yes o No
Valor por omisión	Yes
Descripción	<p>Este parámetro especifica si deben utilizarse tablas de COS mejoradas. Estas tablas asignan pesos razonables a TG de ATM basándose en el coste, velocidad y retardo. Para ATM, el orden de preferencia es:</p> <ul style="list-style-type: none"> • Campus Reserved (SVC o PVC) • Campus Best Effort (SVC o PVC)/WAN reserved PVC • WAN Reserved SVC • WAN Best Effort (SVC o PVC)

Sintaxis:

set high-performance routing

Se le solicitará que entre los valores para los parámetros siguientes. El rango del parámetro se mostrará entre paréntesis (). El valor por omisión del parámetro se mostrará entre corchetes [].

<i>Tabla 6. Lista de parámetros de configuración - Direccionamiento de alto rendimiento (HPR)</i>	
Información de los parámetros	
Parámetro	Maximum sessions for HPR connections
Valores válidos	De 1 a 65535
Valor por omisión	100
Descripción	<p>Este parámetro especifica el número máximo de sesiones permitido en una conexión HPR. Una conexión HPR se define mediante la clase de servicio (COS), la vía de acceso física (TG) y los puntos finales de conexión de la red.</p> <p>Este parámetro sólo se puede aplicar cuando el direccionador es el iniciador del BIND. Si el número de sesiones es superior al valor especificado para este parámetro, HPR asignará otra conexión HPR (RTP).</p>

<i>Tabla 7 (Página 1 de 3). Lista de parámetros de configuración - Temporizador de HPR y opciones de reintento</i>	
Información de los parámetros	
<i>Tráfico con prioridad de transmisión baja</i>	
Parámetro	RTP inactivity timer
Valores válidos	De 1 a 3600 segundos
Valor por omisión	180 segundos
Descripción	<p>Este parámetro especifica el intervalo de inactividad del RTP para conexiones HPR con tráfico con prioridad de transmisión <i>baja</i>. Se trata de una versión de extremo a extremo del temporizador de inactividad LLC, Ti. Si no se produce ninguna recepción durante este intervalo, RTP transmitirá un sondeo. Los períodos de inactividad se supervisan para asegurarse de la integridad de la conexión.</p>
Parámetro	Maximum RTP retries
Valores válidos	De 0 a 10
Valor por omisión	6
Descripción	<p>Este parámetro especifica el número máximo de reintentos antes de que RTP inicie una conmutación de vías de acceso en una conexión HPR que tenga tráfico con prioridad de transmisión baja.</p>
Parámetro	Path switch timer
Valores válidos	De 0 a 7200 segundos
Valor por omisión	180 segundos
Descripción	<p>Este parámetro especifica el tiempo máximo que puede intentarse una conmutación de vías de acceso en una conexión HPR que tenga tráfico con prioridad de transmisión baja. Un valor de cero indica que la función de conmutación de vías de acceso está inhabilitada y que no se realizará la mencionada conmutación.</p>
<i>Tráfico con prioridad de transmisión media</i>	

Mandatos de configuración de APPN

<i>Tabla 7 (Página 2 de 3). Lista de parámetros de configuración - Temporizador de HPR y opciones de reintento</i>	
Información de los parámetros	
Parámetro	RTP inactivity timer
Valores válidos	De 1 a 3600 segundos
Valor por omisión	180 segundos
Descripción	Este parámetro especifica el intervalo de inactividad del RTP para conexiones HPR con tráfico de prioridad de transmisión <i>media</i> . Se trata de una versión de extremo a extremo del temporizador de inactividad LLC, Ti. Si no se produce ninguna recepción durante este intervalo, RTP transmitirá un sondeo. Los períodos de inactividad se supervisan para asegurarse de la integridad de la conexión.
Parámetro	Maximum RTP retries
Valores válidos	De 0 a 10
Valor por omisión	6
Descripción	Este parámetro especifica el número máximo de reintentos antes de que RTP inicie una conmutación de vías de acceso en una conexión HPR que tenga tráfico con prioridad de transmisión <i>media</i> .
Parámetro	Path switch timer
Valores válidos	De 0 a 7200 segundos
Valor por omisión	180 segundos
Descripción	Este parámetro especifica el tiempo máximo que puede intentarse una conmutación de vías de acceso en una conexión HPR que tenga tráfico con prioridad de transmisión <i>media</i> . Un valor de cero indica que la función de conmutación de vías de acceso está inhabilitada y que no se realizará la mencionada conmutación.
<i>Tráfico con prioridad de transmisión alta</i>	
Parámetro	RTP inactivity timer
Valores válidos	De 1 a 3600 segundos
Valor por omisión	180 segundos
Descripción	Este parámetro especifica el intervalo de inactividad del RTP para conexiones HPR con tráfico con prioridad de transmisión <i>alta</i> . Se trata de una versión de extremo a extremo del temporizador de inactividad LLC, Ti. Si no se produce ninguna recepción durante este intervalo, RTP transmitirá un sondeo. Los períodos de inactividad se supervisan para asegurarse de la integridad de la conexión.
Parámetro	Maximum RTP retries
Valores válidos	De 0 a 10
Valor por omisión	6
Descripción	Este parámetro especifica el número máximo de reintentos antes de que RTP inicie una conmutación de vías de acceso en una conexión HPR que tenga tráfico con prioridad de transmisión <i>alta</i> .

<i>Tabla 7 (Página 3 de 3). Lista de parámetros de configuración - Temporizador de HPR y opciones de reintento</i>	
Información de los parámetros	
Parámetro	Path switch timer
Valores válidos	De 0 a 7200 segundos
Valor por omisión	180 segundos
Descripción	Este parámetro especifica el tiempo máximo que puede intentarse una conmutación de vías de acceso en una conexión HPR que tenga tráfico con prioridad de transmisión alta. Un valor de cero indica que la función de conmutación de vías de acceso está inhabilitada y que no se realizará la mencionada conmutación.
<i>Tráfico con prioridad de transmisión de red</i>	
Parámetro	RTP inactivity timer
Valores válidos	De 1 a 3600 segundos
Valor por omisión	180 segundos
Descripción	Este parámetro especifica el intervalo de inactividad del RTP para conexiones HPR con tráfico con prioridad de transmisión de <i>red</i> . Se trata de una versión de extremo a extremo del temporizador de inactividad LLC, Ti. Si no se produce ninguna recepción durante este intervalo, RTP transmitirá un sondeo. Los períodos de inactividad se supervisan para asegurarse de la integridad de la conexión.
Parámetro	Maximum RTP retries
Valores válidos	De 0 a 10
Valor por omisión	6
Descripción	Este parámetro especifica el número máximo de reintentos antes de que RTP inicie una conmutación de vías de acceso en una conexión HPR que tenga tráfico con prioridad de transmisión de red.
Parámetro	Path switch timer
Valores válidos	De 0 a 7200 segundos
Valor por omisión	180 segundos
Descripción	Este parámetro especifica el tiempo máximo que puede intentarse una conmutación de vías de acceso en una conexión HPR que tenga tráfico con prioridad de transmisión de red. Un valor de cero indica que la función de conmutación de vías de acceso está inhabilitada y que no se realizará la mencionada conmutación.

Sintaxis:setdlur

Se le solicitará que entre los valores para los parámetros siguientes. El rango del parámetro se mostrará entre paréntesis (). El valor por omisión del parámetro se mostrará entre corchetes [].

<p><i>Tabla 8 (Página 1 de 4). Lista de parámetros de configuración - Peticionario de LU dependientes</i></p>	
<p>Información de los parámetros</p>	
<p>Parámetro</p>	<p>Enable dependent LU requester (DLUR) on this network node</p>
<p>Valores válidos</p>	<p>Yes, No</p>
<p>Valor por omisión</p>	<p>No</p>
<p>Descripción</p>	<p>Este parámetro especifica si un peticionario de LU dependientes se habilitará funcionalmente en este nodo.</p>
<p>Parámetro</p>	<p>Default fully-qualified CP name of primary DLUS (obligatorio cuando el DLUR está habilitado)</p>
<p>Valores válidos</p>	<p>Una serie con un máximo de 17 caracteres presentados en forma de <i>IDred.nombreCP</i>, donde:</p> <ul style="list-style-type: none"> • <i>IDred</i> es un ID de red de 1 a 8 caracteres • <i>nombreCP</i> es un nombre de CP que tiene entre 1 y 8 caracteres <p>Cada nombre debe respetar las normas siguientes:</p> <ul style="list-style-type: none"> • Primer carácter: De la A a la Z • Del segundo al octavo carácter: De la A a la Z, de 0 a 9 <p>Nota: Sigue dándose soporte a nombres de CP plenamente calificados que usan los caracteres especiales @, \$ y # del juego de caracteres A; no obstante, estos caracteres no deben usarse en los nombres de CP nuevos.</p>
<p>Valor por omisión</p>	<p>Ninguno</p>
<p>Descripción</p>	<p>Este parámetro especifica el nombre del punto de control (CP) plenamente calificado del servidor de LU dependientes (DLUS) que se usa por omisión. El servidor primario por omisión puede alterarse temporalmente en estaciones de trabajo. Este servidor se usa para las solicitudes de entrada de las PU en sentido directo cuando no se ha especificado un DLUS primario para la estación de enlace asociada.</p>
<p>Parámetro</p>	<p>Default fully-qualified CP name of backup dependent LU server (DLUS)</p>
<p>Valores válidos</p>	<p>Una serie con un máximo de 17 caracteres presentados en forma de <i>IDred.nombreCP</i>, donde:</p> <ul style="list-style-type: none"> • <i>IDred</i> es un ID de red de 1 a 8 caracteres • <i>nombreCP</i> es un nombre de CP que tiene entre 1 y 8 caracteres <p>Cada nombre debe respetar las normas siguientes:</p> <ul style="list-style-type: none"> • Primer carácter: De la A a la Z • Del segundo al octavo carácter: De la A a la Z, de 0 a 9 <p>Nota: Sigue dándose soporte a nombres de CP plenamente calificados que usan los caracteres especiales @, \$ y # del juego de caracteres A; no obstante, estos caracteres no deben usarse en los nombres de CP nuevos.</p>
<p>Valor por omisión</p>	<p>Nulo</p>
<p>Descripción</p>	<p>Este parámetro especifica el nombre del punto de control (CP) plenamente calificado del servidor de LU dependientes (DLUS) que se usa como elemento de seguridad por omisión. No se necesita un elemento de seguridad y el valor nulo (que representa la ausencia de entradas) indica la ausencia de un servidor de seguridad por omisión. El servidor de seguridad por omisión puede alterarse temporalmente en estaciones de trabajo.</p>

Tabla 8 (Página 2 de 4). Lista de parámetros de configuración - Peticionario de LU dependientes

Información de los parámetros	
Parámetro	Perform retries to restore disrupted pipe
Valores válidos	Yes, No
Valor por omisión	No
Descripción	<p>Este parámetro especifica si el DLUR intentará restablecer el conducto en un DLUS después de un fallo de éste. Si el DLUR recibe un UNBIND de no interrupción y este parámetro está en No, el DLUR esperará indefinidamente a que un DLUS restablezca el conducto roto. Si el conducto falla por cualquier otra razón y este parámetro está en No, el DLUR intentará alcanzar el DLUS primario una vez. Si no lo consigue, intentará alcanzar el DLUS de seguridad. Si este intento también falla, el DLUR esperará indefinidamente a que un DLUS restablezca el conducto.</p> <p>Consulte "Algoritmo de reintento del DLUR" en la página 42 para obtener una descripción del algoritmo de reintento.</p>
Parámetro	Delay before initiating retries
Valores válidos	De 0 a 2 756 000 segundos
Valor por omisión	120 segundos
Descripción	<p>Este parámetro especifica el tiempo necesario para dos casos diferentes en caso de que se rompa el conducto entre el DLUR y el DLUS.</p> <ul style="list-style-type: none"> En caso de recibir un UNBIND de no interrupción: <p>Este parámetro especifica el tiempo que debe esperar el DLUR antes de intentar alcanzar el DLUS primario. Un valor de 0 indica que el DLUR efectúa un reintento inmediato.</p> En el resto de los casos de fallo del conducto: <p>El DLUR intentará el DLUS primario e, inmediatamente después, el DLUS de seguridad. Si falla, el DLUR esperará el tiempo especificado por el mínimo de <i>short retry timer</i> y el presente parámetro antes de intentar alcanzar el DLUS primario.</p> <p>Consulte "Algoritmo de reintento del DLUR" en la página 42 para obtener una descripción completa del algoritmo de reintento.</p>
Parámetro	Perform short retries to restore disrupted pipe
Valores válidos	Yes, No
Valor por omisión	Si <i>Perform retries to restore disrupted pipes</i> está en Yes, el valor por omisión será Yes. De lo contrario, dicho valor será No.
Descripción	Consulte "Algoritmo de reintento del DLUR" en la página 42 para obtener una descripción completa del algoritmo de reintento.

Mandatos de configuración de APPN

Tabla 8 (Página 3 de 4). Lista de parámetros de configuración - Peticionario de LU dependientes	
Información de los parámetros	
<p>Parámetro Short retry timer</p> <p>Valores válidos De 0 a 2756000 segundos</p> <p>Valor por omisión 120 segundos</p> <p>Descripción En todos los casos de fallo del conducto que no sean un UNBIND de no interrupción, el tiempo mínimo de <i>Delay before initiating retries</i> y el presente parámetro especificarán el tiempo que esperará el DLUR antes de intentar alcanzar el DLUS primario después de que haya fallado un intento de establecer esta conexión.</p> <p>Consulte “Algoritmo de reintento del DLUR” en la página 42 para obtener una descripción completa del algoritmo de reintento.</p>	
<p>Parámetro Short retry count</p> <p>Valores válidos De 0 a 65535</p> <p>Valor por omisión 5</p> <p>Descripción En todos los casos de fallo del conducto que no sean un UNBIND de no interrupción, este parámetro especifica cuantas veces el DLUR intentará realizar reintentos cortos para alcanzar el DLUS después de que haya fallado un intento de establecer esta conexión.</p> <p>Consulte “Algoritmo de reintento del DLUR” en la página 42 para obtener una descripción completa del algoritmo de reintento.</p>	
<p>Parámetro Perform long retries to restore disrupted pipe</p> <p>Valores válidos Yes, No</p> <p>Valor por omisión Si <i>Perform retries to restore disrupted pipes</i> está en Yes, el valor por omisión será Yes. De lo contrario, dicho valor será No.</p> <p>Descripción Consulte “Algoritmo de reintento del DLUR” en la página 42 para obtener una descripción completa del algoritmo de reintento.</p>	
<p>Parámetro Long retry timer</p> <p>Valores válidos De 0 a 2756000 segundos</p> <p>Valor por omisión 300 segundos</p> <p>Descripción Este parámetro especifica el tiempo que esperará el DLUR cuando efectúe reintentos largos.</p> <p>Consulte “Algoritmo de reintento del DLUR” en la página 42 para obtener una descripción completa del algoritmo de reintento.</p>	

Tabla 8 (Página 4 de 4). Lista de parámetros de configuración - Peticionario de LU dependientes

Información de los parámetros	
Parámetro	Take down the dependent link when there is no session
Valores válidos	Yes o No
Valor por omisión	No
Descripción	<p>Este parámetro especifica si el direccionador debe desactivar el enlace con una PU dependiente cuando la PU se desactiva y no hay sesiones activas LU-LU en la misma.</p> <p>Establezca este parámetro en <i>yes</i> si tiene un producto SNA anterior que no da soporte a la recepción de ACTPU a continuación de una DACTPU sin la intervención de una desactivación del enlace. Dicho producto aparecería colgado después de una secuencia de desactivación/activación.</p>

Sintaxis:

set tuning

Se le solicitará que entre los valores para los parámetros siguientes. El rango del parámetro se mostrará entre paréntesis (). El valor por omisión del parámetro se mostrará entre corchetes [].

Nota: Tendrá que reiniciar el sistema para que los cambios que especifique entren en vigor.

Tabla 9 (Página 1 de 6). Lista de parámetros de configuración - Ajuste del nodo APPN

Información de los parámetros	
Parámetro	Maximum number of adjacent nodes
Valores válidos	De 1 a 8000
Valor por omisión	100
Descripción	<p>Este parámetro es un cálculo del número máximo de nodos que espera que sean adyacentes de forma lógica a este nodo de red de direccionador en cualquier momento.</p> <p>El algoritmo de ajuste automático usa este parámetro junto con el parámetro <i>Maximum number of ISR sessions</i> (Número máximo de sesiones de ISR) para calcular los valores de los parámetros <i>Maximum shared memory</i> (Memoria compartida máxima) y <i>Maximum cached directory entries</i> (Número máximo de entradas en el directorio de antememoria).</p> <p>Este parámetro sólo se puede configurar con el Configuration Program.</p>

Mandatos de configuración de APPN

Tabla 9 (Página 2 de 6). Lista de parámetros de configuración - Ajuste del nodo APPN	
Información de los parámetros	
Parámetro	Maximum number of network nodes sharing the same APPN network id
Valores válidos	De 10 a 8000
Valor por omisión	50
Descripción	Este parámetro es un cálculo del número máximo de nodos que espera en la subred (es decir, en la topología conocida por este nodo). Este parámetro sólo se puede configurar con el Configuration Program.
Parámetro	Maximum number of TGs connecting network nodes with the same APPN network id
Valores válidos	De 9 a 64000
Valor por omisión	El valor de <i>maximum number of network nodes in the subnetwork</i> (número máximo de nodos de red en la subred) multiplicado por 3.
Descripción	Este parámetro es un cálculo del número máximo de TG que conectan los nodos de red en la subred (es decir, en la topología conocida por este nodo). Este parámetro sólo se puede configurar con el Configuration Program.
Parámetro	Maximum number of ISR sessions
Valores válidos	De 10 a 60000
Valor por omisión	200
Descripción	Este parámetro especifica un cálculo del número máximo de sesiones de direccionamiento de sesiones intermedias (ISR) al que se espera que dé soporte este nodo de red del direccionador en cualquier momento. El algoritmo de ajuste automático usa este parámetro junto con el del número máximo de nodos adyacentes para calcular los valores de los parámetros de ajuste del número máximo de entradas de directorio en antememoria y el máximo de memoria compartida. Este parámetro sólo se puede configurar con el Configuration Program.
Parámetro	Percent of adjacent nodes with CP-CP sessions using HPR
Valores válidos	De 0 a 100%
Valor por omisión	0 (ninguna)
Descripción	Este parámetro especifica un cálculo del número máximo de EN y NN adyacentes con sesiones de CP-CP que usan el conjunto de opciones 1402 (flujos de control sobre el conjunto de opciones RTP). Este parámetro sólo se puede configurar con el Configuration Program.

<i>Tabla 9 (Página 3 de 6). Lista de parámetros de configuración - Ajuste del nodo APPN</i>	
Información de los parámetros	
Parámetro	Maximum percent of ISR sessions using HPR data connections
Valores válidos	Del 0 al 100 por ciento
Valor por omisión	0 por ciento
Descripción	Este parámetro especifica el porcentaje más elevado de sesiones de ISR que usan correlaciones de ISR a HPR. Este parámetro sólo se puede configurar con el Configuration Program.
Parámetro	Percent adjacent nodes that function as DLUR PU nodes
Valores válidos	Del 0 al 100 por ciento
Valor por omisión	0 por ciento
Descripción	Este parámetro especifica el porcentaje más elevado de nodos adyacentes permitido para funcionar como nodos adyacentes DLUR PU. Este parámetro sólo se puede configurar con el Configuration Program.
Parámetro	Maximum percent ISR sessions used by DLUR LUs
Valores válidos	Del 0 al 100 por ciento
Valor por omisión	0 por ciento
Descripción	Este parámetro especifica el porcentaje más elevado de sesiones de ISR que usan las DLUR LU. Este parámetro sólo se puede configurar con el Configuration Program.
Parámetro	Maximum number of ISR accounting memory buffers
Valores válidos	0 ó 1
Valor por omisión	0 (el valor por omisión es 1 si se activa la contabilidad de sesión ISR)
Descripción	Este parámetro especifica el número máximo de almacenamientos intermedios que se reservarán para la contabilidad de sesiones de ISR. Este parámetro sólo se puede configurar con el Configuration Program.
Parámetro	Maximum memory records per ISR accounting buffer
Valores válidos	De 0 a 2000
Valor por omisión	100
Descripción	Este parámetro especifica el número máximo de registros en memoria por almacenamiento intermedio de contabilidad de ISR. Este parámetro sólo se puede configurar con el Configuration Program.

Mandatos de configuración de APPN

<i>Tabla 9 (Página 4 de 6). Lista de parámetros de configuración - Ajuste del nodo APPN</i>	
Información de los parámetros	
Parámetro	Override tuning algorithm
Valores válidos	Yes, No
Valor por omisión	Yes
Descripción	Cuando se habilita, este parámetro altera temporalmente los cálculos de ajuste generados por los parámetros de entrada de ajuste y le permite especificar valores explícitos para el parámetro Maximum shared memory, el parámetro percent buffer memory y el parámetro Maximum cached directory entries. Este parámetro sólo se puede configurar con el Configuration Program.
Parámetro	Number of local-pus for TN3270E support
Valores válidos	
Valor por omisión	
Descripción	Este parámetro especifica el número de PU locales disponibles para el soporte de TN3270. Este parámetro sólo se puede configurar con el Configuration Program.
Parámetro	Total number of LUs for TN3270E
Valores válidos	
Valor por omisión	
Descripción	Este parámetro especifica el número total de LU disponible para el soporte de TN3270E. Este parámetro sólo se puede configurar con el Configuration Program.

Tabla 9 (Página 5 de 6). Lista de parámetros de configuración - Ajuste del nodo APPN

Información de los parámetros	
Parámetro	Maximum shared memory
Valores válidos	0 - 16777215 KB
Valor por omisión	Configurado automáticamente (configuración basada en la memoria instalada)
Descripción	<p>Este parámetro especifica la cantidad de memoria compartida dentro del direccionador asignada al nodo de red APPN. APPN usa la asignación de memoria compartida para realizar operaciones de red y para mantener las tablas y directorios necesarios.</p> <p>Se puede entrar un valor en Kilobytes o seleccionar que el direccionador escoja un valor por omisión razonable para usos diversos en el momento del arranque en base a la memoria instalada. Tenga en cuenta que el valor por omisión que el direccionador escoja no está basado en el tamaño de la configuración de APPN. Los valores por omisión presuponen que se está ejecutando una red TN3270 o APPN de tamaño medio, además de alguna otra función de direccionamiento no trivial. Puede que el valor por omisión no sea el adecuado si además se configura otra función de direccionador que requiera un uso intensivo de memoria.</p> <p>Al seleccionar el valor <i>auto-configured</i> (configurado automáticamente) en el indicador de línea de mandatos, se puede ver cuál será este valor si se arranca la configuración en el direccionador que se está utilizando. Si se selecciona este valor en el Configuration Program, se debe bajar y activar la configuración para ver el resultado.</p> <p>Este parámetro se puede configurar mediante el Configuration Program y desde la línea de mandatos.</p>
Parámetro	Percent of APPN shared memory to be used for buffers
Valores válidos	De 5 a 50
Valor por omisión	11% o 512 Kilobytes, el valor mayor.
Descripción	<p>Este parámetro especifica la cantidad de memoria compartida que usará APPN para los almacenamientos intermedios.</p> <p>Puede permitir que APPN tenga un tamaño RU de 4 KB estableciendo <i>maximum shared memory</i> en un mínimo de 1 MB y <i>percent of APPN shared memory used for buffers</i> en un valor lo suficientemente grande como para permitir que haya un mínimo de 1 MB de memoria disponible para el gestor de almacenamiento intermedio.</p> <p>Este parámetro se puede configurar mediante el Configuration Program y desde la línea de mandatos.</p>

Mandatos de configuración de APPN

<i>Tabla 9 (Página 6 de 6). Lista de parámetros de configuración - Ajuste del nodo APPN</i>	
Información de los parámetros	
Parámetro	Maximum cached directory entries
Valores válidos	De 0 a 65535
Valor por omisión	4000
Descripción	Este parámetro especifica el número de entradas de directorio que el nodo de red del direccionador almacenará o pondrá en antememoria. Si una entrada de directorio de un nodo se pone en antememoria, el direccionador no necesitará difundir una solicitud de búsqueda para localizarlo. Esto reduce el tiempo necesario para iniciar sesiones con el nodo. Este parámetro se puede configurar mediante el Configuration Program y desde la línea de mandatos.

Sintaxis:

set traces

Se le solicitará que entre los valores para los parámetros siguientes. El rango del parámetro se mostrará entre paréntesis (). El valor por omisión del parámetro se mostrará entre corchetes [].

<i>Tabla 10 (Página 1 de 2). Lista de parámetros de configuración - Preguntas de configuración de los rastreos</i>	
Información de los parámetros	
Parámetro	Turn all trace flags off
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita los distintivos de rastreo.
Parámetro	Edit Node-Level Traces
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Consulte la Tabla 11 en la página 137 para saber cuáles serán las preguntas que se le harán si habilita esta opción.
Parámetro	Edit Interprocess Signals
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Consulte la Tabla 12 en la página 141 para saber cuáles serán las preguntas que se le harán si habilita esta opción.

Tabla 10 (Página 2 de 2). Lista de parámetros de configuración - Preguntas de configuración de los rastreos

Información de los parámetros	
Parámetro	Edit Module Entry and Exit
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Consulte la Tabla 13 en la página 144 para saber cuáles serán las preguntas que se le harán si habilita esta opción.
Parámetro	Edit General
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Consulte la Tabla 14 en la página 146 para saber cuáles serán las preguntas que se le harán si habilita esta opción.

Tabla 11 (Página 1 de 4). Lista de parámetros de configuración - Rastreos de nivel de nodo

Información de los parámetros	
Parámetro	Process management
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos acerca de los procesos de gestión dentro del nodo de red APPN, incluyendo la creación y terminación de procesos, los procesos que entran en un estado de espera y el envío de procesos.
Parámetro	Process to process communication
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos acerca de los mensajes intercambiados entre procesos dentro del nodo de red APPN, incluyendo la puesta en cola y recepción de dichos mensajes.
Parámetro	Locking
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos acerca de los bloqueos obtenidos y liberados en procesos del nodo de red APPN.

Mandatos de configuración de APPN

<i>Tabla 11 (Página 2 de 4). Lista de parámetros de configuración - Rastros de nivel de nodo</i>	
Información de los parámetros	
Parámetro	Miscellaneous tower activities
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos acerca de actividades varias dentro del nodo de red APPN.
Parámetro	I/O to and from the system
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos acerca del flujo de mensajes que entra y sale del nodo de red APPN.
Parámetro	Storage management
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos acerca de la memoria compartida obtenida y liberada por el nodo de red APPN.
Parámetro	Queue data type management
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos acerca de todas las llamadas del nodo de red APPN que gestionan colas de objetivo general.
Parámetro	Table data type management
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos acerca de todas las llamadas del nodo de red APPN que gestionan tablas de objetivo general, incluyendo llamadas para añadir entradas de tabla y llamadas para consultar tablas para entradas específicas.

Tabla 11 (Página 3 de 4). Lista de parámetros de configuración - Rastros de nivel de nodo

Información de los parámetros	
Parámetro	Buffer management
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos acerca de los almacenamientos intermedios del nodo de red APPN que se obtuvieron y liberaron.
Parámetro	Configuration control
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos acerca de las actividades del componente de control de la configuración del nodo de red APPN. Este componente gestiona información sobre los recursos de nodo.
Parámetro	Timer service
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos acerca de las solicitudes de servicio del temporizador desde el nodo de red APPN.
Parámetro	Service provider management
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos acerca de la definición y habilitación o inhabilitación de servicios dentro del nodo de red APPN.
Parámetro	Inter-process message segmenting
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos acerca de la transferencia y liberación de almacenamientos intermedios de mensajes encadenados dentro del nodo de red APPN.

Mandatos de configuración de APPN

<i>Tabla 11 (Página 4 de 4). Lista de parámetros de configuración - Rastros de nivel de nodo</i>	
Información de los parámetros	
Parámetro	Control of processes outside scope of this tower
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos acerca de la definición y activación de procesos externos al nodo de red APPN como cuando el recurso de operador del nodo (NOF) define el control de la configuración de procesos externos.
Parámetro	Monitoring existence of processes, services, towers
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos acerca de las solicitudes que inician o detienen la supervisión de procesos o servicios dentro del nodo de red APPN.
Parámetro	Distributed environment control
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos acerca de las solicitudes dentro del nodo de red APPN que definen subsistemas y crean entornos.
Parámetro	Process to service dialogs
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos acerca de todas las llamadas del nodo de red APPN que abren, cierran o envían datos en un diálogo.
Parámetro	AVL Tree Support
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, la opción de rastreo hace que el recurso de rastreo del direccionador reúna datos acerca de todas las llamadas que gestionan árboles AVL.

Tabla 12 (Página 1 de 4). Lista de parámetros de configuración - Rastreo de señales entre procesos

Información de los parámetros	
Parámetro	Address space manager
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de señales entre procesos, del componente del gestor de espacios de direcciones.
Parámetro	Attach manager
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de señales entre procesos, del componente del gestor de conexiones.
Parámetro	Configuration services
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de señales entre procesos, del componente de servicios de configuración.
Parámetro	Dependent LU requester
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de señales entre procesos, del componente de peticionario de LU dependientes.
Parámetro	Directory services
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de señales entre procesos, del componente de servicios de directorio.

Mandatos de configuración de APPN

<i>Tabla 12 (Página 2 de 4). Lista de parámetros de configuración - Rastros de señales entre procesos</i>	
Información de los parámetros	
Parámetro	Half Session
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de señales entre procesos, del componente de semisesión.
Parámetro	HPR Path Control
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de señales entre procesos, del componente de control de la vía de acceso HPR.
Parámetro	LUA RUI
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de señales entre procesos, del componente LUA RUI.
Parámetro	Management Services
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de señales entre procesos, del componente de servicios de gestión.
Parámetro	Node Operator Facility
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de señales entre procesos, del componente de recurso del operador de nodo.

Tabla 12 (Página 3 de 4). Lista de parámetros de configuración - Rastreo de señales entre procesos

Información de los parámetros	
Parámetro	Path Control
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de señales entre procesos, del componente de control de las vías de acceso.
Parámetro	Presentation Services
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de señales entre procesos, del componente de servicios de presentación.
Parámetro	Resource manager
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de señales entre procesos, del componente de gestor de recursos.
Parámetro	Session connector manager
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de señales entre procesos, del gestor del conector de sesiones.
Parámetro	Session connector
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de señales entre procesos, del conector de sesiones.

Mandatos de configuración de APPN

<i>Tabla 12 (Página 4 de 4). Lista de parámetros de configuración - Rastreo de señales entre procesos</i>	
Información de los parámetros	
Parámetro	Session manager
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de señales entre procesos, del gestor de sesiones.
Parámetro	Session services
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de señales entre procesos, del componente de servicios de sesión.
Parámetro	Topology and routing services
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de señales entre procesos, de los servicios de topología y direccionamiento.

<i>Tabla 13 (Página 1 de 3). Lista de parámetros de configuración - Rastreo de la entrada y salida en módulos</i>	
Información de los parámetros	
Parámetro	Attach manager
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de la entrada y salida en módulos del gestor de conexiones.
Parámetro	Half session
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, el parámetro indica al recurso de rastreo que incluya datos de rastreo de la entrada y salida en módulos del componente de semisesión.

<i>Tabla 13 (Página 2 de 3). Lista de parámetros de configuración - Rastros de la entrada y salida en módulos</i>	
Información de los parámetros	
Parámetro	LUA RUI
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de entrada y salida en módulos del componente LUA RUI.
Parámetro	Node operator facility
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, el parámetro indica al recurso de rastreo que incluya datos de rastreo de entrada y salida en módulos del recurso del operador de nodos.
Parámetro	Presentation services
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, el parámetro indica al recurso de rastreo que incluya datos de rastreo de la entrada y salida en módulos de los servicios de presentación.
Parámetro	Rapid transport protocol
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, el parámetro indica al recurso de rastreo que incluya datos de rastreo de la entrada y salida en módulos del componente de protocolo de transporte rápido.
Parámetro	Resource manager
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de la entrada y salida en módulos del gestor de recursos.

Mandatos de configuración de APPN

Tabla 13 (Página 3 de 3). Lista de parámetros de configuración - Rastros de la entrada y salida en módulos

Información de los parámetros	
Parámetro	Session manager
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de la entrada y salida en módulos del gestor de sesiones.

Tabla 14 (Página 1 de 4). Lista de parámetros de configuración - Rastros de nivel de componentes generales

Información de los parámetros	
Parámetro	Accounting services
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de información general de los servicios de contabilidad.
Parámetro	Address space manager
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de información general del gestor de espacios de direcciones.
Parámetro	Architected transaction programs
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de información general del componente de los programas de transacciones arquitecturadas.
Parámetro	Configuration services
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de información general de los servicios de configuración.

Tabla 14 (Página 2 de 4). Lista de parámetros de configuración - Rastros de nivel de componentes generales

Información de los parámetros	
Parámetro	Dependent LU requester
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de información general del peticionario de LU dependientes.
Parámetro	Directory services
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de información general de los servicios de directorio.
Parámetro	HPR path control
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de información general del control de vías de acceso HPR.
Parámetro	LUA RUI
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de información general del componente LUA RUI.
Parámetro	Management services
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de información general de los servicios de gestión.

Mandatos de configuración de APPN

<i>Tabla 14 (Página 3 de 4). Lista de parámetros de configuración - Rastros de nivel de componentes generales</i>	
Información de los parámetros	
Parámetro	Node operator facility
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de información general del recurso del operador de nodo.
Parámetro	Path control
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de información general del control de vías de acceso.
Parámetro	Problem determination services
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de información general del servicio de determinación de problemas.
Parámetro	Rapid transport protocol
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de información general del control del transporte rápido.
Parámetro	Session connector manager
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de información general del gestor del conector de sesiones.

Tabla 14 (Página 4 de 4). Lista de parámetros de configuración - Rastreo de nivel de componentes generales

Información de los parámetros	
Parámetro	Session connector
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de información general del conector de sesiones.
Parámetro	Session services
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de información general de los servicios de sesión.
Parámetro	SNMP subagent
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de información general del subagente SNMP.
Parámetro	TN3270E Server
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de información general del servidor de TN3270E.
Parámetro	Topology and routing services
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita esta opción de rastreo de APPN. Cuando se habilita, este parámetro indica al recurso de rastreo que incluya datos de rastreo de información general de los servicios de topología y direccionamiento.

Mandatos de configuración de APPN

Tabla 15 (Página 1 de 2). Lista de parámetros de configuración - Rastreo varios	
Información de los parámetros	
<p>Parámetro Data link control transmissions and receptions</p> <p>Valores válidos Yes, No</p> <p>Valor por omisión No</p> <p>Descripción Si se habilita este parámetro, el recurso de rastreo de APPN rastreará todos los XID y PIU que el nodo APPN transmita y reciba.</p>	
<p>Parámetro Trace RTP Headers</p> <p>Valores válidos Yes, No</p> <p>Valor por omisión No</p> <p>Descripción Si se activa este parámetro, el recurso de rastreo de APPN rastreará todas las cabeceras de los flujos de RTP. Esta opción está disponible sólo si Data link control transmissions and receptions es <i>yes</i>.</p>	
<p>Parámetro Include payload in RTP trace</p> <p>Valores válidos Yes, No</p> <p>Valor por omisión No</p> <p>Descripción Si se activa este parámetro, el recurso de rastreo de APPN rastreará los datos de carga útil de los flujos de RTP. Esta opción está disponible sólo si trace RTP headers es <i>yes</i>.</p>	
<p>Parámetro Filter the Data</p> <p>Valores válidos Yes, No</p> <p>Valor por omisión No</p> <p>Descripción Si se activa este parámetro, el recurso de rastreo de APPN filtrará los datos de rastreo según la forma en que responda a las preguntas siguientes.</p>	
<p>Parámetro Truncate the data</p> <p>Valores válidos Yes, No</p> <p>Valor por omisión No</p> <p>Descripción Si se activa este parámetro, el recurso de rastreo de APPN truncará los datos de rastreo. Se le solicitará que especifique la <i>longitud a rastrear</i></p>	
<p>Parámetro Length to trace</p> <p>Valores válidos De 1 a 3600</p> <p>Valor por omisión 100</p> <p>Descripción Este parámetro especifica el número de bytes de datos de rastreo a acumular.</p>	
<p>Parámetro Trace Locates</p> <p>Valores válidos Yes, No</p> <p>Valor por omisión No</p> <p>Descripción Si se activa este parámetro, el recurso de rastreo de APPN rastreará las localizaciones.</p>	

<i>Tabla 15 (Página 2 de 2). Lista de parámetros de configuración - Rastreo varios</i>	
Información de los parámetros	
Parámetro	Trace TDU
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Si se activa este parámetro, el recurso de rastreo de APPN rastreará las actualizaciones de datos topológicos.
Parámetro	Trace route setups
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Si se activa este parámetro, el recurso de rastreo de APPN rastreará las configuraciones de ruta.
Parámetro	Trace CP Capabilities
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Si se activa este parámetro, el recurso de rastreo de APPN rastreará las posibilidades de rastreo del CP.
Parámetro	Trace Session Control
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Si se activa este parámetro, el recurso de rastreo de APPN rastreará el tráfico de control de sesiones.
Parámetro	Trace XID
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Si se activa este parámetro, el recurso de rastreo de APPN rastreará los XID.

Sintaxis:

set management

Se le solicitará que entre los valores para los parámetros siguientes. El rango del parámetro se mostrará entre paréntesis (). El valor por omisión del parámetro se mostrará entre corchetes [].

Mandatos de configuración de APPN

Tabla 16 (Página 1 de 2). Lista de parámetros de configuración - Gestión de nodos APPN	
Información de los parámetros	
Parámetro	Collect intermediate session information
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro especifica si el nodo APPN debe reunir datos sobre las sesiones intermedias que pasan por el nodo (contadores de sesión y características de sesión). Los datos se capturan en variables SNMP MIB para APPN.
Parámetro	Save RSCV information for intermediate sessions
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro especifica si el nodo APPN debe guardar el vector de control de selección de ruta (RSCV) para una sesión intermedia. Los datos se capturan en una variable asociada SNMP MIB para APPN. El RSCV de sesión se transporta en la solicitud BIND usada para activar una sesión entre dos LU. Describe la ruta óptima a través de una red APPN de una sesión LU-LU determinada. El RSCV de sesión contiene los nombres de CP y TG asociados con cada par de nodos adyacentes situados a lo largo de una ruta que va de un nodo de origen a uno de destino.
Parámetro	Create intermediate session records
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita la creación de registros de datos para sesiones intermedias que pasan a través de este nodo. Los registros contienen información sobre contadores de sesiones y características de las sesiones. También se incluye la información de RSCV en los registros de datos si está habilitado el parámetro Save RSCV information for intermediate sessions. Si este parámetro está en yes, el valor de <i>collect intermediate session information</i> se alterará temporalmente.
Parámetro	Record creation threshold
Valores válidos	De 0 a 4294967, en incrementos de 1 KB
Valor por omisión	0
Descripción	Este parámetro especifica un umbral de bytes para crear registros de sesión intermedios. Cuando los datos de sesión superan el valor de este contador de bytes en una cantidad par múltiplo, se crea un registro.

Tabla 16 (Página 2 de 2). Lista de parámetros de configuración - Gestión de nodos APPN

Información de los parámetros	
Parámetro	Held alert queue size
Valores válidos	De 0 a 255
Valor por omisión	10
Descripción	Este parámetro establece el tamaño de la cola de alertas retenidas configurable. Esta cola se usa para guardar las alertas de APPN antes de enviarlas a un punto focal. Si la cola se desborda, se descartarán las alertas más antiguas.

Tabla 17 (Página 1 de 2). Lista de parámetros de configuración - Soportes de registro de APPN ISR

Información de los parámetros	
<i>Parámetros de memoria</i>	
Parámetro	Memory (consulte las notas de tabla)
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro habilita o inhabilita la captación de datos de sesiones intermedias en la memoria local del direccionador.
Parámetro	Maximum memory buffers
Valores válidos	Del 0 al 1
Valor por omisión	1
Descripción	Este parámetro especifica el número de almacenamientos intermedios que se asignarán en la memoria local del direccionador para almacenar registros de sesiones intermedias.
Parámetro	Maximum memory records per buffer
Valores válidos	De 0 a 2000
Valor por omisión	100
Descripción	Este parámetro especifica el número máximo de registros de sesiones intermedias que pueden almacenarse en el almacenamiento intermedio de memoria del direccionador.
Parámetro	Memory buffers full
Valores válidos	Stop recording (Dejar de registrar) (0), Wrap (Acomodar) (1)
Valor por omisión	Dejar de registrar (0)
Descripción	Este parámetro especifica la acción que debe seguirse cuando el almacenamiento intermedio de memoria asignado para almacenar registros de sesiones intermedias se llena. Seleccione Stop recording (Dejar de registrar) para indicar al direccionador que descarte cualquier registro de sesión intermedia nuevo. Seleccione Wrap (Acomodar) para permitir que los registros nuevos sobrescriban registros ya existentes en el almacenamiento intermedio. Primero se sobrescribirán los registros más antiguos del almacenamiento intermedio.

Mandatos de configuración de APPN

<i>Tabla 17 (Página 2 de 2). Lista de parámetros de configuración - Soportes de registro de APPN ISR</i>	
Información de los parámetros	
Parámetro	Memory record format
Valores válidos	ASCII (0), Binary (Binario) (1)
Valor por omisión	ASCII (0)
Descripción	Este parámetro especifica el formato en que los registros de sesiones intermedias se almacenarán en la memoria local del direccionador.
Parámetro	Time between database updates
Valores válidos	De 60 a 1440 minutos
Valor por omisión	60
Descripción	Este parámetro establece el tiempo, en minutos, entre actualizaciones de base de datos topológica.
Nota:	
<ul style="list-style-type: none">• Cuando habilita la captación de registros de sesiones intermedias, los datos asociados a los registros también se captan, por omisión, en SNMP• Variables MIB para APPN. En tal caso, las variables MIB se actualizarán, independientemente de que el parámetro de captación de información de sesiones intermedias (en la Tabla 16 en la página 152) se haya habilitado.• Los datos de sesiones intermedias pueden almacenarse en la memoria del direccionador.	

Add

Use el mandato **add** para añadir o actualizar:

Sintaxis:

add port

Se le solicitará que entre los valores para los parámetros siguientes. El rango del parámetro se mostrará entre paréntesis (). El valor por omisión del parámetro se mostrará entre corchetes [].

<i>Tabla 18 (Página 1 de 4). Lista de parámetros de configuración - Configuración de puertos</i>	
Información de los parámetros	
Parámetro	Link type
Valores válidos	Ethernet (E) Red en anillo (T) ATM (A) DLSw (D) PPP (P) Frame relay (F) SDLC (S) X.25 (X) IP
Valor por omisión	Ninguno
Descripción	Este parámetro especifica el tipo de enlace asociado a este puerto.
Parámetro	Interface number
Valores válidos	De 0 a 65533
Valor por omisión	0
Descripción	Este parámetro define el número de interfaz física de la interfaz de hardware a la que está conectado este dispositivo.
Parámetro	Port name
Valores válidos	Serie que tiene entre 1 y 8 caracteres, donde el primer carácter es alfabético y del 2 al 8 los caracteres son alfanuméricos.
Valor por omisión	Un nombre único no calificado que se genera automáticamente. El nombre estará formado por: <ul style="list-style-type: none"> • TR (red en anillo) • EN (Ethernet) • DLS (DLSw) • IP255 • ATM • FR (Frame Relay) • X25 (X.25) • SDLC (SDLC) • PPP (punto a punto) • IP seguido del número de la interfaz.
Descripción	Puede cambiar el nombre de puerto por un nombre de su elección. Este parámetro especifica el nombre que representa este puerto.
Parámetro	Enable APPN routing on this port
Valores válidos	Yes, No
Valor por omisión	Yes
Descripción	Este parámetro especifica si el direccionamiento de APPN debe habilitarse en este puerto.

Tabla 18 (Página 2 de 4). Lista de parámetros de configuración - Configuración de puertos	
Información de los parámetros	
<p>Parámetro Support multiple PU</p> <p>Valores válidos Yes, No</p> <p>Valor por omisión No</p> <p>Descripción Este parámetro especifica si el puerto dará soporte a varias subáreas.</p>	
<p>Parámetro Service any node</p> <p>Valores válidos Yes, No</p> <p>Valor por omisión Yes</p> <p>Descripción Este parámetro especifica cómo responde el nodo de red del direccionador a una solicitud de otro nodo para establecer una conexión sobre este puerto. Cuando se habilita este parámetro, el nodo de red acepta cualquier solicitud que reciba de otro nodo para establecer conexión. Cuando se inhabilita este parámetro, el nodo de red acepta las solicitudes de conexión únicamente de los nodos que haya definido explícitamente (mediante definiciones de estaciones de enlace). Esta opción proporciona un nivel añadido de seguridad al nodo de red del direccionador.</p> <p>Nota: Cuando se inhabilita este parámetro, sólo se aceptan las solicitudes de conexión de un nodo adyacente si el parámetro del nombre del CP plenamente calificado del nodo se ha configurado para una estación de enlace definida en este puerto.</p> <p>Cuando este parámetro está habilitado (valor por omisión), puede que siga deseando que este nodo de red pueda iniciar conexiones con nodos específicos sobre este puerto.</p>	
<p>Parámetro Treat non-configured callers as LEN nodes</p> <p>Valores válidos Yes, No</p> <p>Valor por omisión No</p> <p>Descripción Este parámetro especifica si APPN debe tratar a los llamantes del nodo de red dinámico que no solicitan sesiones CP-CP como nodos LEN. Es aplicable sólo si service any node es yes.</p> <p>Si este parámetro es yes:</p> <ul style="list-style-type: none"> • el direccionador trata al nodo adyacente como nodo LEN independientemente del tipo de nodo del XID3 que se ha recibido • el direccionador envía los XID3 afirmando que el direccionador es un nodo LEN (un EN sin sesión CP-CP ni soporte HPR) 	
<p>Parámetro High-performance routing (HPR) supported</p> <p>Valores válidos Yes, No</p> <p>Valor por omisión Yes para puertos de red en anillo, Ethernet, Frame Relay y PPP.</p> <p>Descripción Este parámetro indica si las estaciones de enlace de este puerto darán soporte a HPR. El valor puede alterarse temporalmente en la definición de la estación de enlace.</p>	

Tabla 18 (Página 3 de 4). Lista de parámetros de configuración - Configuración de puertos	
Información de los parámetros	
Parámetro	IPv4 Precedence
Valores válidos	Yes o No
Valor por omisión	No
Descripción	Este parámetro establece el valor de precedencia de IPv4, lo que permite el filtro de precedencia BRS de los paquetes encapsulados IPv4.
Parámetro	Limited Resource (únicamente PPP y FR sobre circuitos de marcación)
Valores válidos	Yes, No
Valor por omisión	Si el circuito de marcación es <i>bajo pedido</i> , el valor por omisión será Yes. De lo contrario, dicho valor será No.
Descripción	Este parámetro especifica si las estaciones de enlace de este puerto son un recurso limitado. El valor puede alterarse temporalmente en la definición de la estación de enlace.
Parámetro	Support bridged formatted frames (sólo Frame relay)
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro especifica si el puerto de Frame Relay dará soporte a las tramas formateadas puenteadas. Si está configurando Frame Relay para que dé soporte al formato puenteadado, también necesitará configurar un identificador de nodo frontera.
Parámetro	Boundary node identifier (sólo Frame Relay)
Valores válidos	De X'0000 0000 0001' a X'7FFF FFFF FFFF'
Valor por omisión	X'4FFF 0000 0000'
Descripción	Este parámetro especifica la dirección del MAC del identificador del nodo frontera. El direccionador usa esta dirección del MAC para reconocer que la trama es una trama puenteadada de Frame Relay destinada a APPN.
Parámetro	Subnet visit count
Valores válidos	De 1 a 255
Valor por omisión	El valor por omisión se toma del parámetro de nivel de nodo equivalente
Descripción	Este parámetro especifica el valor por omisión de este puerto para el número máximo de subredes que puede atravesar una sesión de varias subredes. Nota: Esta pregunta sólo se hace si la función de nodo de frontera está habilitada en este nodo.

Mandatos de configuración de APPN

<i>Tabla 18 (Página 4 de 4). Lista de parámetros de configuración - Configuración de puertos</i>	
Información de los parámetros	
Parámetro	Adjacent node subnet affiliation
Valores válidos	<ul style="list-style-type: none"> • 0 (nativa) • 1 (no nativa) • 2 (negociable)
Valor por omisión	2
Descripción	Este parámetro especifica el valor por omisión de todos los enlaces a través de este puerto así como si el nodo adyacente está en la subred APPN nativa de este nodo o en una subred APPN no nativa. Un valor de 2 instruye al nodo para que negocie en el momento de activación del enlace para determinar si la estación de enlace adyacente es nativa o no.
	Nota: Esta pregunta sólo se hace si la función de nodo de frontera está habilitada en este nodo.

<i>Tabla 19 (Página 1 de 5). Lista de parámetros de configuración - Configuración de puerto para ATM</i>	
Información de los parámetros	
Parámetro	Local ATM Address
Valores válidos	Cualquier serie de 14 caracteres hexadecimales
Valor por omisión	Ninguno
Descripción	Este parámetro especifica la serie de 7 bytes que incluye la parte del usuario de la dirección ATM local. La parte del usuario es el ESI de 6 bytes y el campo del selector de 1 byte. Esta parte del usuario debe ser única en relación con la parte de la red de la dirección ATM, que se recupera del adaptador de ATM. El selector debe ser único para cada tipo de protocolo.
Parámetro	Enable incoming calls
Valores válidos	Yes o No
Valor por omisión	Yes
Descripción	Este parámetro determina si se rechazarán las llamadas en el nivel de ATM.
Parámetro	ATM Network Type
Valores válidos	Campus o Widearea
Valor por omisión	Campus
Descripción	Este parámetro especifica el tipo de red usado para los valores por omisión para las redes de conexiones y otras estaciones de enlace definidas en este puerto.

<i>Tabla 19 (Página 2 de 5). Lista de parámetros de configuración - Configuración de puerto para ATM</i>	
Información de los parámetros	
Parámetro	Shareable connection network traffic
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro especifica si el tráfico de red de conexión puede direccionarse en el ATM VC configurado para una estación de enlace de este puerto.
Parámetro	Shareable other protocol traffic
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro especifica si otro tráfico de protocolo de mayor nivel puede direccionarse en el ATM VC configurado para una estación de enlace de este puerto.
Parámetro	Broadband Bearer Class
Valores válidos	Clase_A, Clase_C, Clase_X
Valor por omisión	Clase_X
Descripción	Este parámetro especifica la clase de portador solicitada desde la red ATM. Las clases se definen: <p>Clase A Velocidad de bit constante (CBR) con requisitos de tiempo de extremo a extremo</p> <p>Clase C Velocidad de bit variable (VBR) sin requisitos de tiempo de extremo a extremo</p> <p>Clase X Servicio que permite el tipo de tráfico definido por el usuario y requisitos de tiempo</p>
Parámetro	Best Effort Indicator
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro indica si se requiere una garantía completa en este SVC. Si el valor de este parámetro es <i>yes</i> , los VCC asociados a esta interfaz se asignarán basándose en la anchura de banda disponible.
Nota: Los parámetros siguientes son parámetros de tráfico de reenvío.	
Parámetro	Forward Traffic Peak Cell Rate
Valores válidos	Del 1 al 85% de velocidad de línea
Valor por omisión	Capacidad efectiva por omisión del puerto/48
Descripción	Este parámetro indica un límite superior en la velocidad de transmisión de células.

Mandatos de configuración de APPN

<i>Tabla 19 (Página 3 de 5). Lista de parámetros de configuración - Configuración de puerto para ATM</i>	
Información de los parámetros	
Parámetro	Forward Traffic Sustained Cell Rate
Valores válidos	Del 1 al 85% de velocidad de línea
Valor por omisión	Capacidad efectiva por omisión del puerto/48
Descripción	Este parámetro indica un límite superior en la velocidad media de transmisión de células. No puede especificar este parámetro si está usando la conexión de Mejor esfuerzo.
Parámetro	Forward Traffic Tagging
Valores válidos	Yes, No
Valor por omisión	Yes
Descripción	Este parámetro indica que las células que no cumplen la especificación de tráfico de prioridad 0 de pérdida de células, pero sí que cumplen la especificación de tráfico de prioridad 1 de dicha pérdida se marcan y pueden entrar en la red ATM. No puede especificar este parámetro si está usando la conexión de Mejor esfuerzo.
Parámetro	Forward QoS
Valores válidos	CLASS_0, CLASS_1, CLASS_2, CLASS_3, CLASS_4, donde
	CLASS_0 Clase sin especificar. La red no especifica ninguna QoS.
	CLASS_1 El rendimiento es comparable al de la línea privada digital actual.
	CLASS_2 Clase destinada al vídeo y audio en paquetes para las aplicaciones multimedia y de videoconferencia.
	CLASS_3 Clase destinada al interfuncionamiento de protocolos orientados a la conexión como, por ejemplo, Frame Relay.
	CLASS_4 Clase destinada al interfuncionamiento de protocolos sin conexión como, por ejemplo, IP.
Valor por omisión	CLASS_0
Descripción	Este parámetro indica qué clase de servicio se proporciona a una conexión virtual ATM. Este parámetro siempre es CLASS_0 para una conexión Best Effort (mejor esfuerzo).
Nota: Los parámetros siguientes son parámetros de tráfico hacia atrás.	
Parámetro	Backward Traffic Peak Cell Rate
Valores válidos	Del 1 al 85% de velocidad de línea
Valor por omisión	Capacidad efectiva por omisión del puerto/48
Descripción	Este parámetro indica un límite superior en la velocidad de transmisión de células.

<i>Tabla 19 (Página 4 de 5). Lista de parámetros de configuración - Configuración de puerto para ATM</i>	
Información de los parámetros	
Parámetro	Backward Traffic Sustained Cell Rate
Valores válidos	Del 1 al 85% de velocidad de línea
Valor por omisión	Capacidad efectiva por omisión del puerto/48
Descripción	Este parámetro indica un límite superior en la velocidad media de transmisión de células. No puede especificar este parámetro para una conexión de Mejor esfuerzo.
Parámetro	Backward Traffic Tagging
Valores válidos	Yes, No
Valor por omisión	Yes, a menos que se tenga una conexión de Mejor esfuerzo
Descripción	Este parámetro indica que las células que no cumplen la especificación de tráfico de prioridad 0 de pérdida de células, pero sí que cumplen la especificación de tráfico de prioridad 1 de dicha pérdida se marcan y pueden entrar en la red ATM. No puede especificar este parámetro para una conexión de Mejor esfuerzo.
Parámetro	Backward QoS
Valores válidos	CLASS_0, CLASS_1, CLASS_2, CLASS_3, CLASS_4, donde
	CLASS_0 Clase sin especificar. La red no especifica ninguna QoS.
	CLASS_1 El rendimiento es comparable al de la línea privada digital actual.
	CLASS_2 Clase destinada al vídeo y audio en paquetes para las aplicaciones multimedia y de videoconferencia.
	CLASS_3 Clase destinada al interfuncionamiento de protocolos orientados a la conexión como, por ejemplo, Frame Relay.
	CLASS_4 Clase destinada al interfuncionamiento de protocolos sin conexión como, por ejemplo, IP.
Valor por omisión	CLASS_0
Descripción	Este parámetro indica qué clase de servicio se proporciona a una conexión virtual ATM. No puede especificar este parámetro para una conexión de Mejor esfuerzo.
Parámetro	Callout Anonymously
Valores válidos	Yes, No
Valor por omisión	no
Descripción	Este parámetro indica si APPN pasará la dirección de origen cuando llame.

<i>Tabla 19 (Página 5 de 5). Lista de parámetros de configuración - Configuración de puerto para ATM</i>	
Información de los parámetros	
Parámetro	LDLC retry count
Valores válidos	De 1 a 255
Valor por omisión	3
Descripción	Este parámetro se usa junto con el período del temporizador LDLC para proporcionar una entrega fiable de XID. La cuenta de reintentos se inicializa cuando un mandato o solicitud se transmite por primera vez sobre un enlace. Si el período del temporizador LDLC se agota antes de recibir una respuesta, se volverá a transmitir el mandato o solicitud, la cuenta de reintentos disminuirá y el período del temporizador LDLC se reiniciará. Si el temporizador agota el tiempo con la cuenta de reintentos en 0, se presupondrá que el enlace no es operativo.
Parámetro	LDLC Timer Period
Valores válidos	De 1 a 255 segundos
Valor por omisión	Para ATM: 1 segundo Para IP: 15 segundos
Descripción	Este parámetro especifica el período de tiempo usado con LDLC retry count .

Tabla 20 (Página 1 de 4). Lista de parámetros de configuración - Definición de puertos

Información de los parámetros	
Parámetro	Maximum BTU size
Valores válidos	<p>De 768 a 1496 bytes para Ethernet</p> <p>De 768 a 17745 bytes para red en anillo</p> <p>De 768 a 4096 bytes para ATM</p> <p>De 768 a 4096 bytes para IP</p> <p>De 768 a 8136 bytes para Frame Relay</p> <p>De 768 a 8132 bytes para Frame Relay sobre RDSI y V.25bis</p> <p>De 768 a 4086 bytes para PPP</p> <p>De 768 a 4082 bytes para PPP sobre RDSI y V.25bis</p> <p>X.25 tomará el valor del nivel de red</p> <p>De 768 a 2048 bytes para todos los demás puertos</p>
Valor por omisión	<p>1289 bytes para Ethernet</p> <p>2048 bytes para red en anillo</p> <p>2048 para ATM</p> <p>1469 bytes para IP</p> <p>2048 bytes para Frame Relay o PPP</p> <p>2044 bytes para Frame Relay o PPP sobre RDSI y V.25bis</p> <p>2048 bytes para SDLC</p> <p>X.25 tomará el valor del nivel de red</p>
Descripción	<p>Este parámetro especifica el número de bytes de la unidad de transmisión básica (BTU) más grande que puede procesar (transmitida o recibida) una estación de enlace definida en este puerto.</p> <p>Nota: Si se recibe un BIND negociable con un tamaño de RU superior a 2048, normalmente el dispositivo elegirá un tamaño de RU máximo de 2048. Si se recibe un BIND no negociable con un tamaño de RU superior a 2048, el dispositivo dará soporte al tamaño de RU más grande, hasta un tamaño máximo de 4096.</p>
Parámetro	Maximum number of link stations
Valores válidos	<p>De 1 a 127 para puertos SDLC</p> <p>De 1 a 65535 para todos los demás puertos</p>
Valor por omisión	
Descripción	<p>Si SDLC está configurado como multipunto y primario, este parámetro tendrá un valor por omisión de 127.</p> <p>Este parámetro especifica el número máximo de estaciones de enlace que podrán usar este puerto. Este parámetro permite que los recursos del nodo APPN y este puerto se restrinjan.</p>

<i>Tabla 20 (Página 2 de 4). Lista de parámetros de configuración - Definición de puertos</i>	
Información de los parámetros	
Parámetro	Percent of link stations reserved for incoming calls (únicamente Ethernet, red en anillo, FR, X.25)
Valores válidos	De 0 a 100
	La suma del porcentaje de las estaciones de enlace reservadas para las llamadas de entrada y el porcentaje de estaciones de enlace reservadas para las llamadas de salida no puede superar el 100%.
Valor por omisión	0
Descripción	Este parámetro especifica el porcentaje del número máximo de estaciones de enlace que se reservará para las llamadas de entrada. Las estaciones de enlace que no se reserven para llamadas de entrada o de salida estarán disponibles para ambos objetivos según la demanda.
Parámetro	Percent of link stations reserved for outgoing calls
Valores válidos	De 0 a 100
	La suma del porcentaje de las estaciones de enlace reservadas para las llamadas de entrada y el porcentaje de estaciones de enlace reservadas para las llamadas de salida no puede superar el 100%. Si SDLC es primario y multipunto, el valor válido será 100.
Valor por omisión	0 Si SDLC es primario y multipunto, el valor por omisión será 100.
Descripción	Este parámetro especifica el porcentaje del número máximo de estaciones de enlace que se reservará para las llamadas de salida. Las fracciones resultado del cálculo se truncarán. Las estaciones de enlace que no se reserven para llamadas de entrada o de salida estarán disponibles para ambos objetivos según la demanda.
Parámetro	UDP port number for XID exchange
Valores válidos	De 1024 a 65535
Valor por omisión	11000
Descripción	Este parámetro especifica el número de puerto UDP que se usará para el intercambio de XID y que se usa durante la definición de puerto IP. Este número de puerto debe ser el mismo que el definido en otros dispositivos de la red.
Parámetro	UDP port number for network priority traffic
Valores válidos	De 1024 a 65535
Valor por omisión	11001
Descripción	Este parámetro especifica el número de puerto UDP que se usará para el tráfico de prioridad de red.
Parámetro	UDP port number for high priority traffic
Valores válidos	De 1024 a 65535
Valor por omisión	11002
Descripción	Este parámetro especifica el número de puerto UDP que se usará para tráfico de alta prioridad.

<i>Tabla 20 (Página 3 de 4). Lista de parámetros de configuración - Definición de puertos</i>	
Información de los parámetros	
Parámetro	UDP port number for medium priority traffic
Valores válidos	De 1024 a 65535
Valor por omisión	11003
Descripción	Este parámetro especifica el número de puerto UDP que se usará para tráfico de prioridad media.
Parámetro	UDP port number for low priority traffic
Valores válidos	De 1024 a 65535
Valor por omisión	11004
Descripción	Este parámetro especifica el número de puerto UDP que se usará para el tráfico de baja prioridad.
Parámetro	IP network type
Valores válidos	Campus o Widearea
Valor por omisión	Widearea
Descripción	Este parámetro especifica el tipo de red IP.
Parámetro	Local APPN SAP address
Valores válidos	Múltiplos de cuatro en el rango hexadecimal incluido entre X'04' y X'EC'
Valor por omisión	X'04'
Descripción	Este parámetro especifica la dirección de SAP local que se usará para las comunicaciones con las estaciones de enlace de APPN definidas en este puerto.
Parámetro	Local HPR SAP address (sólo para Ethernet y redes en anillo)
Valores válidos	Múltiplos de cuatro en el rango hexadecimal incluido entre X'04' y X'EC'
Valor por omisión	X'C8'
Descripción	Este parámetro indica el punto de acceso de servicio local que se usará para las comunicaciones con las estaciones de enlace HPR definidas en este puerto.

<i>Tabla 20 (Página 4 de 4). Lista de parámetros de configuración - Definición de puertos</i>	
Información de los parámetros	
Parámetro	Branch uplink
Valores válidos	Yes o No
Valor por omisión	No
Descripción	<p>Este parámetro indica si el valor por omisión de las estaciones de enlace que usan este puerto será hacia arriba o hacia abajo. Si se especifica <i>yes</i>, las estaciones de enlace que usen este puerto darán como valor por omisión para Branch uplink <i>yes</i>.</p> <p>Notas:</p> <ol style="list-style-type: none">1. Esta pregunta sólo se hace si el parámetro de nivel de nodo Enabled Branch Extender está en <i>yes</i>.2. Si Branch uplink está en <i>yes</i>, Branch Extender presentará su apariencia de nodo final a esta estación de enlace. De lo contrario, Branch Extender presentará su apariencia de nodo de red.3. Por lo general, Branch uplink se establece en <i>yes</i> para nodos de red conectados a una WAN y no para nodos de red conectados a una LAN.

Tabla 21 (Página 1 de 6). Lista de parámetros de configuración - Características del TG del puerto por omisión

Información de los parámetros	
Parámetro	Cost per connect time
Valores válidos	De 0 a 255
Valor por omisión	
	Para SVC ATM:
	Campus ATM best effort (Mejor esfuerzo de campus ATM) 0
	Campus ATM reserved (Reservado a campus ATM) 64
	WAN ATM best effort (Mejor esfuerzo de WAN ATM) 0
	WAN ATM reserved (Reservado a WAN ATM) 128
	Para PVC ATM:
	Campus ATM best effort (Mejor esfuerzo de campus ATM) 0
	Campus ATM reserved (Reservado a campus ATM) 0
	WAN ATM best effort (Mejor esfuerzo de WAN ATM) 0
	WAN ATM reserved (Reservado a WAN ATM) 0
	Para IP: 0 para Campus y WAN
Descripción	<p>Para el resto: 0</p> <p>Este parámetro especifica el coste por característica de TG del tiempo de conexión para todas las estaciones de enlace de este puerto.</p> <p>El coste por característica de TG dle tiempo de conexión expresa el coste relativo de mantener una conexión sobre el TG asociado. Las unidades están definidas por el usuario y normalmente se basan en las tarifas aplicables del recurso de transmisión que se está usando. Los valores asignados deben reflejar el gasto real del mantenimiento de una conexión sobre el TG en relación con el resto de los TG de la red. Un valor de cero significa que las conexiones sobre el TG pueden establecerse sin ningún coste adicional (como en el caso de varios de los recursos no conmutados). Los valores más altos representan costes más altos.</p>

<i>Tabla 21 (Página 2 de 6). Lista de parámetros de configuración - Características del TG del puerto por omisión</i>	
Información de los parámetros	
Parámetro	Cost per byte
Valores válidos	De 0 a 255
Valor por omisión	
	Para SVC ATM y PVC ATM:
	Campus ATM best effort (Mejor esfuerzo de campus ATM) 0
	Campus ATM reserved (Reservado a campus ATM) 0
	WAN ATM best effort (Mejor esfuerzo de WAN ATM) 128
	WAN ATM reserved (Reservado a WAN ATM) 0
	Para IP: 0 para Campus y WAN
	Para el resto: 0
Descripción	Este parámetro especifica la característica de TG de coste por byte de todas las estaciones de enlace definidas en este puerto. La característica de TG de coste por byte expresa el coste relativo de transmitir un byte sobre un TG asociado. Las unidades están definidas por el usuario y el valor asignado debe reflejar los gastos reales de transmisión sobre el TG en relación con el resto de TG de la red. Un valor de cero significa que los bytes pueden transmitirse sobre el TG sin costes adicionales. Los valores más altos representan costes más altos.

Tabla 21 (Página 3 de 6). Lista de parámetros de configuración - Características del TG del puerto por omisión

Información de los parámetros	
Parámetro	Security
Valores válidos	<p>Nonsecure (no fiable) el resto (por ejemplo, conectado por satélite o localizado en un país no fiable).</p> <p>Public switched network (Red conmutada pública) fiable en el sentido de que la ruta no se determina previamente</p> <p>Underground cable (Cable subterráneo) situado en un país fiable (determinado por el administrador de red)</p> <p>Secure conduit (Conducto fiable) Sin guardar, (por ejemplo, conducto presurizado)</p> <p>Guarded conduit (Conducto guardado) protegido contra las intervenciones físicas</p> <p>Encrypted (Cifrado) se proporciona un cifrado de nivel de enlace</p> <p>Guarded radiation (Radiación vigilada) conducto vigilado que contiene el medio de transmisión; protegido contra la intervención de radiación y la intervención física</p>
Valor por omisión	<p>Para SVC ATM y PVC ATM:</p> <p>Campus ATM best effort (Mejor esfuerzo de campus ATM) Nonsecure (no fiable)</p> <p>Campus ATM reserved (Reservado a campus ATM) Nonsecure (no fiable)</p> <p>WAN ATM best effort (Mejor esfuerzo de WAN ATM) Public switched network (Red conmutada pública)</p> <p>WAN ATM reserved (Reservado a WAN ATM) Public switched network (Red conmutada pública)</p> <p>Para IP:</p> <p>Campus Nonsecure (no fiable)</p> <p>WAN Public switched network (Red conmutada pública)</p>
Descripción	<p>Para el resto: Nonsecure (No fiable)</p> <p>Este parámetro especifica la característica de TG de seguridad de todas las estaciones de enlace definidas en este puerto. Esta característica indica el nivel de protección de seguridad asociada al TG. Si se necesitan atributos de seguridad que no sean los definidos arquitecturalmente, puede usarse una de las características de TG definidas por el usuario para especificar valores adicionales.</p>

Tabla 21 (Página 4 de 6). Lista de parámetros de configuración - Características del TG del puerto por omisión

Información de los parámetros	
Parámetro	Propagation delay
Valores válidos	
	Minimum LAN (LAN mínima) menos de 480 microsegundos
	Telephone (Teléfono) entre 0,48 y 49,152 milisegundos
	Packet switched (Paquete conmutado) entre 49,152 y 245,76 milisegundos
	Satellite (Satélite) superior al máximo de 245,76 milisegundos
Valor por omisión	
	Para SVC ATM y PVC ATM:
	Campus ATM best effort (Mejor esfuerzo de campus ATM) Telephone (Teléfono)
	Campus ATM reserved (Reservado a campus ATM) Minimum LAN
	WAN ATM best effort (Mejor esfuerzo de WAN ATM) Packet switched (Paquete conmutado)
	WAN ATM reserved (Reservado a WAN ATM) Telephone (Teléfono)
	Para IP:
	Campus Telephone (Teléfono)
	WAN Packet switched (Paquete conmutado)
Descripción	Este parámetro especifica la característica del TG del retardo de propagación de todas las estaciones de enlace definidas en este puerto. Esta característica especifica el rango aproximado de tiempo que tarda una señal en propagarse de un extremo del TG al otro.

Tabla 21 (Página 5 de 6). Lista de parámetros de configuración - Características del TG del puerto por omisión

Información de los parámetros	
Parámetro	Effective capacity
Valores válidos	2 dígitos hexadecimales del rango incluido entre X'00' y X'FF'
Valor por omisión	<p>FR: X'45' (64 kbps) PPP: X'45' (64 kbps) DLSw: X'75' (4 Mbps) SDLC: X'45' (64 kbps) X.25: X'45' (64 kbps) TR: X'85' (16 Mbps) TR: X'75' (4 Mbps) ENET: X'80' (10 Mbps)</p> <p>Para SVC ATM (25 Mbps) y PVC ATM (25Mbps): Campus ATM best effort: X'8A' Campus ATM reserved: X'8A' WAN ATM best effort: X'8A' WAN ATM reserved: X'8A'</p> <p>Para IP: Campus: X'75' WAN: X'43'</p>
Descripción	<p>Este parámetro especifica la característica de TG de capacidad efectiva para todas las conexiones asociadas (TG) de este puerto.</p> <p>Este parámetro especifica la velocidad de transmisión de bits máxima para los enlaces físicos y los lógicos. Observe que la capacidad efectiva de un enlace lógico puede ser inferior a la velocidad de enlace físico. La velocidad está representada en los archivos COS como un número de coma flotante codificado en un único byte con unidades de 300 bps. La capacidad efectiva está codificada como representación de un único byte. Los valores X'00' y X'FF' son casos especiales usados para denotar las capacidades mínima y máxima. El rango de codificación es muy amplio; no obstante, sólo se pueden especificar 256 valores del rango.</p> <p>Este parámetro proporciona el valor por omisión del parámetro de capacidad efectiva en la opción Modify TG Characteristics Command Line (Línea de mandatos de modificación de las características de TG). Esta opción le permite alterar temporalmente los valores por omisión .* asignados a características de TG en las estaciones de enlace individuales que defina.</p>

Mandatos de configuración de APPN

<i>Tabla 21 (Página 6 de 6). Lista de parámetros de configuración - Características del TG del puerto por omisión</i>	
Información de los parámetros	
Parámetro	First user-defined TG characteristic
Valores válidos	De 0 a 255
Valor por omisión	128
Descripción	<p>Este parámetro especifica la primera característica de TG definida por el usuario para todas las estaciones de enlace definidas en este puerto.</p> <p>Esta primera característica especifica la primera de tres características adicionales que pueden definir los usuarios para describir los TG de una red. El valor por omisión de 128 permite definir un subconjunto de TG como más o menos deseable que el resto sin tener que definir valores para todos los TG.</p>
Parámetro	Second user-defined TG characteristic
Valores válidos	De 0 a 255
Valor por omisión	128
Descripción	<p>Este parámetro especifica la segunda característica de TG definida por el usuario para todas las estaciones de enlace definidas en este puerto.</p> <p>Esta segunda característica especifica la segunda de tres características adicionales que pueden definir los usuarios para describir los TG de una red.</p>
Parámetro	Third user-defined TG characteristic
Valores válidos	De 0 a 255
Valor por omisión	128
Descripción	<p>Este parámetro especifica la tercera característica de TG definida por el usuario para todas las estaciones de enlace definidas en este puerto.</p> <p>Esta tercera característica especifica la tercera de tres características adicionales que pueden definir los usuarios para describir los TG de una red.</p>

<i>Tabla 22 (Página 1 de 4). Lista de parámetros de configuración - Características LLC del puerto por omisión</i>	
Información de los parámetros	
Parámetro	Remote APPN SAP
Valores válidos	Múltiplos de cuatro en el rango hexadecimal incluido entre X'04' y X'EC'
Valor por omisión	X'04'
Descripción	Este parámetro especifica el SAP asociado a la estación de enlace de APPN del nodo adyacente.

Tabla 22 (Página 2 de 4). Lista de parámetros de configuración - Características LLC del puerto por omisión

Información de los parámetros	
Parámetro	Maximum number of outstanding I-format LPDUs (TW)
Valores válidos	De 1 a 127
Valor por omisión	26
Descripción	<p>Este parámetro especifica el número máximo de LLC de LPDU (TW) de formato I pendientes para todas las estaciones de enlace de este puerto.</p> <p>El número máximo de LPDU de formato I pendientes define la opción de transmisión de la línea de mandatos (TW) que es el número máximo de LPDU de formato I numeradas secuencialmente que la estación de enlace puede tener pendientes de acuse de recibo.</p>
Parámetro	Receive window size
Valores válidos	De 1 a 127
Valor por omisión	26
Descripción	<p>Este parámetro especifica el tamaño de la opción LLC receive Command Line (RW) de todas las estaciones de enlace de este puerto.</p> <p>El parámetro RW especifica el número máximo de LPDU de formato I numeradas secuencialmente y sin acuse de recibo que puede recibir la estación de enlace de la estación de enlace remota. RW se notifica en tramas SNA XID y tramas IEEE 802.2 XID. El receptor XID debe establecer el TW efectivo en un valor inferior o igual al del RW recibido a fin de evitar desbordamientos.</p>
Parámetro	Inactivity timer (Ti)
Valores válidos	De 1 a 254 segundos
Valor por omisión	30 segundos
Descripción	<p>Este parámetro especifica el temporizador de inactividad (Ti) de LLC de todas las estaciones de enlace de este puerto.</p> <p>Una estación de enlace LLC usa el Ti para detectar una condición no operativa en la estación de enlace remota o en el soporte de transmisión. Si no se recibe una LPDU en el intervalo de tiempo especificado por el Ti, se transmitirá una LPDU de mandato de formato S con bit de sondeo para solicitar el estado de la estación de enlace remota. La recuperación se basará en el temporizador de respuesta (T1).</p>

Tabla 22 (Página 3 de 4). Lista de parámetros de configuración - Características LLC del puerto por omisión

Información de los parámetros	
Parámetro	Reply timer (T1)
Valores válidos	De 1 a 254 segundos
Valor por omisión	2 segundos
Descripción	<p>Este parámetro especifica el temporizador de respuesta LLC (T1) de todas las estaciones de enlace de este puerto.</p> <p>Una estación de enlace LLC usa T1 para detectar un fallo en la recepción de un acuse de recibo necesario o una respuesta de la estación remota de enlace. Cuando T1 se agota, la estación de enlace envía una unidad de datos de protocolo de la capa de enlace (LPDU) de mandato de formato S con el bit de sondeo establecido, para solicitar el estado de la estación de enlace remota o cualquier LPDU de mandato de formato U que no haya recibido respuesta. La duración de T1 debe tener en cuenta cualquier retardo introducido en las capas inferiores.</p>
Parámetro	Maximum number of retransmissions (N2)
Valores válidos	De 1 a 254
Valor por omisión	8
Descripción	<p>Este parámetro especifica el número máximo de retransmisiones (N2) de todas las estaciones de enlace de este puerto.</p> <p>El parámetro N2 especifica el número máximo de veces que se retransmitirá una LPDU después de la expiración del temporizador de respuesta (T1).</p>
Parámetro	Receive acknowledgment timer (T2)
Valores válidos	De 1 a 254, calculado en décimas de segundo
Valor por omisión	1
Descripción	<p>Este parámetro especifica el temporizador de acuse de recibo de LLC (T2) de todas las estaciones de enlace de este puerto.</p> <p>Puede usarse el parámetro T2 con el contador N3 para reducir el tráfico de acuse de recibo. Una estación de enlace usa T2 para retrasar el envío de un acuse de recibo de una LPDU de formato I recibida. T2 se inicia cuando se recibe una LPDU de formato I y se restablece cuando se envía un acuse de recibo en una LPDU de formato I o formato S. Si T2 expira, la estación de enlace deberá enviar un acuse de recibo tan pronto como sea posible. El valor de T2 debe ser inferior al de T1, para asegurarse de que la estación de enlace remota reciba el acuse de recibo retrasado antes de que expire su T1.</p>

Tabla 22 (Página 4 de 4). Lista de parámetros de configuración - Características LLC del puerto por omisión

Información de los parámetros	
Parámetro	Acknowledgments needed to increment working window
Valores válidos	De 0 a 127
Valor por omisión	1
Descripción	Cuando la ventana de trabajo (Ww) no es igual al tamaño máximo de la ventana de transmisión (Maximum Transmit Window Size - Tw), este parámetro será la cantidad de LPDU de formato I transmitidas cuyo acuse de recibo debe efectuarse antes de poder incrementar la ventana de trabajo (en 1). Cuando se detecta una congestión, por la pérdida de LPDU de formato I, Ww se establece en 1.

Tabla 23. Lista de parámetros de configuración - Valores por omisión de la alteración temporal de HPR

Información de los parámetros	
Parámetro	Inactivity timer override for HPR (HPR Ti)
Valores válidos	De 1 a 254 segundos
Valor por omisión	2 segundos
Descripción	Este parámetro especifica el temporizador de inactividad de LLC (HPR Ti) que se usará para todas las estaciones de enlace de este puerto que den soporte a HPR cuando el parámetro de soporte de HPR esté habilitado en dicho puerto. Este valor por omisión alterará temporalmente el valor del parámetro del temporizador de inactividad (Ti) del LLC especificado en el parámetro de las características del LLC por omisión.
Parámetro	Reply timer override for HPR (HPR T1)
Valores válidos	De 1 a 254 segundos
Valor por omisión	2 segundos
Descripción	Este parámetro especifica el temporizador de respuesta del LLC (HPR T1) que se usará en todas las estaciones de enlace de este puerto que den soporte a HPR, cuando el parámetro de HPR con soporte esté habilitado en él. Este valor por omisión altera temporalmente el valor del parámetro del temporizador de respuesta del LLC (T1) especificado en el parámetro de las características del LLC por omisión.
Parámetro	Maximum number of retransmissions for HPR (HPR N2)
Valores válidos	De 1 a 254
Valor por omisión	3
Descripción	Este parámetro especifica el número máximo de retransmisiones (HPR N2) de LLC que se va a usar para todas las estaciones de enlace de este puerto que den soporte a HPR, cuando el parámetro de HPR con soporte esté habilitado en este puerto. Este valor por omisión altera temporalmente el valor por omisión del parámetro del número máximo de LLC de retransmisiones (N2) por omisión especificado en el parámetro de las características del LLC por omisión.

Sintaxis:

Mandatos de configuración de APPN

add

link-station

Se le solicitará que entre los valores para los parámetros siguientes. El rango del parámetro se mostrará entre paréntesis (). El valor por omisión del parámetro se mostrará entre corchetes [].

Información de los parámetros	
Parámetro	Does link support APPN function
Valores válidos	Yes o No
Valor por omisión	Yes
Descripción	<p>Este parámetro especifica si esta estación de enlace dará soporte a la función de APPN.</p> <p>Si la respuesta es <i>no</i>, no se harán preguntas sobre sesiones de CP-CP, seguridad, codificación, nombre de CP, tipo de nodo adyacente, branch extender y nodo de frontera ampliado (Extended Border Node) y todas estas funciones se inhabilitarán. Además, se inhabilitará HPR y no se hará ninguna pregunta de HPR.</p>
Parámetro	Link station name (obligatorio)
Valores válidos	<p>Una serie de 1 a 8 caracteres:</p> <ul style="list-style-type: none"> • Primer carácter: De la A a la Z • Del segundo al octavo carácter: De la A a la Z, de 0 a 9
Valor por omisión	Ninguno
Descripción	Este parámetro especifica el nombre de una estación de enlace que representa el TG (enlace) entre el nodo de red del direccionador y el nodo adyacente. El nombre de la estación de enlace debe ser único en este nodo de red.
Parámetro	Port name
Valores válidos	<p>Un nombre único no calificado que se genera automáticamente.</p> <p>El nombre estará formado por:</p> <ul style="list-style-type: none"> • TR (red en anillo) • EN (Ethernet) • DLS (DLSw) • FR (Frame Relay) • X25 (X.25) • SDLC (SDLC) • PPP (punto a punto) • IP <p>seguido del número de la interfaz.</p>
Valor por omisión	El nombre del puerto en el que está definida esta estación de enlace.
Descripción	Este parámetro especifica el nombre que representa al puerto en el que está definida esta estación de enlace. El puerto debe estar ya configurado para APPN.

Tabla 24 (Página 2 de 10). Lista de parámetros de configuración - Estaciones de enlace - Detalle

Información de los parámetros	
Parámetro	Tipo de enlace (únicamente X.25 y ATM)
	Si <i>limited resource</i> = yes está configurado para esta estación de enlace, entonces el parámetro del tipo de enlace tendrá como valor por omisión un valor de 1 (SVC) y no se podrá configurar.
Valores válidos	Si es PVC, especifique un número de canal lógico dentro del rango incluido entre 1 y 4095 Si es SVC, especifique una dirección del DTE cuya longitud variable puede alcanzar los 15 dígitos
Valor por omisión	0, a menos que sea un recurso limitado.
Descripción	Este parámetro especifica si el enlace X.25 es un PVC o SVC.
Parámetro	MAC address of adjacent node (obligatorio) (únicamente formato puenteado Ethernet, de red en anillo, DLSw y FR)
Valores válidos	Puertos de red en anillo y DLSw: <ul style="list-style-type: none"> 12 dígitos hexadecimales dentro del rango incluido entre X'000000000001' y X'7FFFFFFFFF' Puertos de Ethernet/802.3: <ul style="list-style-type: none"> 12 dígitos hexadecimales con formato X' xyxxxxxxxx' donde: x es cualquier dígito hexadecimal y es un dígito hexadecimal del juego {0, 2, 4, 6, 8, A, C, E}
Valor por omisión	Ninguno
Descripción	Este parámetro especifica la dirección de la capa de control de acceso al soporte (MAC) del nodo adyacente. Se usan formatos diferentes para red en anillo y Ethernet/802.3. Puertos de red en anillo y DLSw: La dirección del MAC se especifica en formato no canónico. En el formato de dirección no canónico, el bit de cada octeto que se transmitirá en primer lugar se representa como el bit más significativo. Puertos de Ethernet/802.3: La dirección del MAC se especifica en formato canónico. En el formato de dirección canónico, el bit de cada octeto que se transmitirá en primer lugar se representa como el bit menos significativo.
Parámetro	IP address of adjacent node (Enterprise Extender only)
Valores válidos	Cualquier dirección IP válida
Valor por omisión	ninguno
Descripción	Cada enlace del puerto HPR/IP debe tener una dirección de IP de destino única.

Tabla 24 (Página 3 de 10). Lista de parámetros de configuración - Estaciones de enlace - Detalle

Información de los parámetros	
Parámetro	Adjacent node type
Valores válidos	APPN network node (nodo de red APPN), APPN end node (nodo final APPN) y LEN end node (nodo final LEN)
Valor por omisión	Nodo de red APPN
Descripción	<p>Este parámetro identifica si el nodo adyacente es un nodo APPN, un nodo final (LEN) de red de entrada baja.</p> <p>Cuando se selecciona <i>APPN end node</i> y <i>Limited resource</i> está en No, APPN cambia el tipo de nodo adyacente internamente para <i>aprender</i> y trabaja con cualquier tipo de nodo.</p> <p>Si selecciona <i>APPN end node</i> y <i>Limited resource</i> está en Yes, el tipo de nodo adyacente permanecerá igual.</p> <p>Cuando seleccione <i>LEN end node</i>, el parámetro del nombre del punto de control plenamente calificado es obligatorio. Si este nodo de red está comunicando con el producto IBM Virtual Telecommunications Access Method (VTAM) a través del nodo LEN y éste no es un nodo T2.1 o no tiene un nombre de punto de control (CP) definido explícitamente, el número de XID del nodo de red del direccionador para el parámetro de conexión de subárea también debe especificarse para establecer una conexión.</p> <p>Nota: <i>LEN end node</i> (Nodo final de red) no es un tipo de nodo válido para la interfaz HPR/IP.</p>
Parámetro	XID node identification
Valores válidos	Serie de 8 dígitos hexadecimales (0-F)
Valor por omisión	X'00000000'
Descripción	<p>Este parámetro especifica los campos bloque de ID y número de ID que identifican el nodo adyacente. Es aplicable sólo cuando el campo Adjacent node type está establecido en <i>LEN end node</i>. Si selecciona <i>yes</i> para replace inbound XID3 CP name and XID with configured values, el valor de este campo substituirá los parámetros correspondientes del XID recibido.</p>

Tabla 24 (Página 4 de 10). Lista de parámetros de configuración - Estaciones de enlace - Detalle

Información de los parámetros	
Parámetro	fully-qualified CP name of adjacent node
Valores válidos	<p>Una serie con un máximo de 17 caracteres presentados en forma de <i>IDred.nombreCP</i>, donde:</p> <ul style="list-style-type: none"> <i>IDred</i> es un ID de red de 1 a 8 caracteres <i>nombreCP</i> es un nombre de punto de control que tiene entre 1 y 8 caracteres <p>Cada nombre debe respetar las normas siguientes:</p> <ul style="list-style-type: none"> Primer carácter: De la A a la Z Del segundo al octavo carácter: De la A a la Z, de 0 a 9 <p>Nota: Sigue dándose soporte a nombres de CP plenamente calificados que usan los caracteres especiales @, \$ del juego de caracteres A; no obstante, estos caracteres no deben usarse en los nombres de CP nuevos.</p>
Valor por omisión	Ninguno
Descripción	<p>Este parámetro especifica el nombre del CP plenamente calificado del nodo adyacente. Para los casos en que este parámetro no sea obligatorio, el nombre del CP del nodo adyacente puede saberse dinámicamente durante el intercambio de XID; no obstante, si se especifica un nombre de CP, éste debe coincidir con la definición del nodo adyacente para que el enlace se active satisfactoriamente.</p> <p>Nota: Este parámetro es obligatorio cuando se produce una de las situaciones siguientes:</p> <ul style="list-style-type: none"> El parámetro <i>Service any node</i> está en Disable (inhabilitar). El parámetro <i>Adjacent node type</i> está en LEN end node. El parámetro <i>CP-CP session level security</i> está en Enable (Habilitar). El enlace es un recurso limitado.
Parámetro	Replace inbound XID3 CP name and XID with configured values
Valores válidos	Yes o No
Valor por omisión	No
Descripción	<p>Este parámetro especifica si el direccionador debe alterar temporalmente los parámetros id de nodo y nombre de CP recibidos en los XID de un nodo LEN configurado. Es aplicable sólo cuando el campo adjacent node type está establecido en <i>LEN end node</i>.</p> <p>Si tiene un gran número de nodos LEN que no están configurados adecuadamente para participar en una red APPN completa, se puede configurar la identidad de los mismos en el direccionador y que el direccionador altere temporalmente los valores de los XID correspondientes antes de reenviar dichos XID.</p>

Tabla 24 (Página 5 de 10). Lista de parámetros de configuración - Estaciones de enlace - Detalle	
Información de los parámetros	
Parámetro	Activate link automatically
	Si es un recurso limitado, este parámetro se establece en No y no se podrá configurar.
Valores válidos	Yes, No
Valor por omisión	Yes
Descripción	Cuando se activa este parámetro, el nodo de red del direccionador activa automáticamente el enlace con el nodo adyacente e inicia una conexión.
Parámetro	Retry link activation unconditionally
Valores válidos	Yes, No
Valor por omisión	No
Descripción	<p>Este parámetro especifica si el direccionador siempre debe intentar reactivar el enlace independientemente del motivo de la anomalía del enlace. Es aplicable sólo para enlaces capacitados para marcación de salida donde activate link automatically es yes.</p> <p>Normalmente si un enlace no consigue iniciarse o cae debido a algún suceso que no es un mandato del operador, el direccionador elige selectivamente si va a reactivarlo. Si la causa de la anomalía puede requerir la reconfiguración de uno de los dos nodos, el direccionador no reinicia el enlace automáticamente. Esto evita una repetición periódica (con registro cronológico, alertas, etc.) del intento de conexión no satisfactorio. Si desea alterar temporalmente este comportamiento y hacer que los enlaces siempre intenten efectuar la reconexión, seleccione yes para este parámetro.</p>
Parámetro	Allow CP-CP sessions on this link
Valores válidos	Yes, No
Valor por omisión	Yes, si el tipo de nodo adyacente es un nodo de red APPN o un nodo final APPN. No para el resto de tipos de nodo adyacente
Descripción	<p>Este parámetro especifica si las sesiones entre puntos de control se activarán sobre esta estación de enlace.</p> <p>Este parámetro permite controlar el establecimiento de sesiones de CP-CP entre nodos de red adyacentes para que la carga asociada con las actualizaciones de base de datos de topología (TDU) se restrinja.</p> <p>Nota: Cada nodo de red APPN debe tener, como mínimo, una sesión de CP-CP establecida en otro nodo de red APPN a fin de mantener la conectividad mínima necesaria para actualizar la base de datos topológica. Además, es posible que se necesite más que la conectividad mínima para eliminar puntos aislados de fallo y para mejorar la dinámica de la red.</p>

<i>Tabla 24 (Página 6 de 10). Lista de parámetros de configuración - Estaciones de enlace - Detalle</i>	
Información de los parámetros	
Parámetro	CP-CP session level security
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro especifica si la seguridad de nivel de sesión se aplica a sesiones de CP-CP establecidas sobre esta estación de enlace. Cuando se habilita la seguridad de nivel de sesión, se intercambian datos cifrados y se comparan durante los flujos BIND (lo que incluye el BIND, la respuesta al BIND y una RU de seguridad FMH-12). Para establecer satisfactoriamente una sesión de CP-CP con la seguridad de nivel de sesión habilitada, los dos asociados deben estar configurados con la misma clave de cifrado. Actualmente, el soporte de la seguridad de nivel de sesión se limita al protocolo de verificación de LU-LU básico.
Parámetro	Encryption key
Valores válidos	Hasta 16 dígitos hexadecimales. Si se especifican menos de 16 dígitos, se rellena el espacio de la derecha del valor con ceros.
Valor por omisión	Ninguno
Descripción	Este parámetro se usa para codificar los datos intercambiados durante los flujos BIND. Para establecer una sesión de CP-CP, los dos asociados deben estar configurados con la misma clave.
Parámetro	Use enhanced session security (Si está habilitada la seguridad)
Valores válidos	Yes, No
Valor por omisión	No
Parámetro	High-performance routing (HPR) supported
Valores válidos	Yes, No
Valor por omisión	APPN network node (nodo de red APPN), APPN end node (nodo final APPN) o LEN end node (nodo final LEN): el valor especificado en el parámetro de HPR con soporte por omisión para este puerto. El resto de tipos de nodo adyacentes: No
Descripción	Este parámetro indica si esta estación de enlace da soporte a HPR. El usuario deberá inhabilitar el soporte a HPR si el enlace subyacente no es fiable. No se establecerá una conexión HPR a menos que ambas estaciones de enlace anuncien su soporte a HPR durante el intercambio de XID.
Parámetro	DLCI number for link (únicamente Frame Relay)
Valores válidos	De 16 a 1007
Valor por omisión	16
Descripción	El parámetro DLCI identifica la conexión de enlace de datos lógicos de frame-relay con el nodo adyacente.

Mandatos de configuración de APPN

Tabla 24 (Página 7 de 10). Lista de parámetros de configuración - Estaciones de enlace - Detalle	
Información de los parámetros	
Parámetro	Station address of adjacent node (únicamente SDLC)
Valores válidos	Una dirección que esté incluida dentro del rango (1 - FE)
Valor por omisión	C1
Descripción	Este parámetro especifica la dirección del nodo adyacente.
Parámetro	Limited Resource (PPP, X.25 FR sobre circuitos de marcación, ATM)
Valores válidos	Yes o No
Valor por omisión	No
Descripción	Si el <i>link type</i> (tipo de enlace) es PPP o FR, el valor por omisión se tomará del parámetro <i>limited resource</i> para el puerto asociado. Este parámetro especifica si el TG para esta estación de enlace es un recurso limitado. Si responde <i>yes</i> , el Virtual Channel Type (Tipo de canal virtual) será <i>SVC</i> .
Parámetro	Branch uplink
Valores válidos	Yes o No
Valor por omisión	El valor especificado para Branch Uplink en el puerto.
Descripción	Este parámetro indica si este enlace será un enlace hacia la rama de arriba (a WAN) o hacia abajo (a LAN). Esta pregunta sólo se hace si se ha establecido Enabled Branch Extender en <i>yes</i> y si esta estación de enlace no es un nodo de red. Si Enabled Branch Extender está en <i>yes</i> y esta estación de enlace es un nodo de red, Branch Uplink tendrá como valor por omisión <i>yes</i> .
Parámetro	Is uplink to another Branch Extender node
Valores válidos	Yes o No
Valor por omisión	No
Descripción	Este parámetro indica si el nodo adyacente tiene la función de Branch Extender habilitada. Esta pregunta sólo se hace si Branch Extender está habilitado en este nodo, se trata de un enlace hacia arriba y dicho enlace es un recurso limitado.

Tabla 24 (Página 8 de 10). Lista de parámetros de configuración - Estaciones de enlace - Detalle

Información de los parámetros	
Parámetro	Preferred Network Node Server
Valores válidos	Yes o No
Valor por omisión	No
Descripción	<p>Este parámetro indica si este enlace hacia arriba es un servidor de nodos de red que debe utilizarse como servidor de nodos de red del nodo que da soporte a la función Branch Extender y actúa como nodo final. Si se especifica <i>yes</i>, este enlace hacia arriba se usará como servidor de nodos de red de este nodo.</p> <p>Esta pregunta sólo se hará si:</p> <ul style="list-style-type: none"> • Enabled Branch Extender está en <i>yes</i>, • Esta estación es un nodo de red. • Branch Uplink está en <i>yes</i> y • las sesiones de CP-CP tienen soporte en este enlace.
Parámetro	TG Number
Valores válidos	<p>Si <i>limited resource</i> está en <i>Yes</i>, los valores válidos estarán incluidos entre 1 y 20. Si <i>limited resource</i> está en <i>No</i> y <i>link type</i> (tipo de enlace) es X.25 SVC, los valores válidos estarán incluidos entre 0 y 20.</p> <p>De lo contrario, estarán incluidos entre 0 y 20.</p>
Valor por omisión	<p>Si <i>limited resource</i> está en <i>Yes</i>, el valor por omisión será 1. Si <i>limited resource</i> está en <i>NO</i>, el valor por omisión será 0.</p> <p>De lo contrario, el valor por omisión es 0.</p>
Descripción	Este parámetro identifica de forma única un TG entre nodos adyacentes.
Parámetro	Solicit SSCP session
Valores válidos	Yes o No
Valor por omisión	No
Descripción	<p>Si el parámetro link station name (nombre de la estación de enlace) es el mismo que CP name (nombre del CP), el valor por omisión será <i>yes</i>.</p> <p>Este parámetro indica si este enlace va a solicitar sesiones de SSCP.</p>
Parámetro	Local Node ID
Valores válidos	5 dígitos hexadecimales
Valor por omisión	X'00000'
Descripción	Este parámetro especifica el identificador de nodo local que representa la PU dependiente local ante VTAM. Esta pregunta sólo se efectúa si Solicit SSCP session es <i>yes</i> . El id del nodo local debe ser único.

Tabla 24 (Página 9 de 10). Lista de parámetros de configuración - Estaciones de enlace - Detalle	
Información de los parámetros	
Parámetro	Enable Host Initiated Dynamic LU Definition
Valores válidos	Yes o No
Valor por omisión	No
Descripción	<p>Este parámetro indica si las LU dependientes se crearán dinámicamente (en oposición a tener que configurarlas). Si se especifica yes, las LU se definirán para esta PU a medida que se reciban solicitudes ACTLU (con CV0E). Con esta función, no es necesario configurar las LU para el servidor de TN3270E.</p> <p>Nota: Esta pregunta sólo se efectúa si Solicit SSCP session es yes.</p>
Parámetro	Pool Name for Host-initiated Dynamic LUs
Valores válidos	<p>Una serie de 1 a 8 caracteres:</p> <ul style="list-style-type: none"> • Primer carácter: De la A a la Z, \$, #, @, ó < • Del segundo al octavo carácter: De la A a la Z, de 0 a 9, \$, #, @, >, ó <
Valor por omisión	Ninguno
Descripción	<p>Este parámetro especifica el nombre de una agrupación que se creará para contener las LU que el sistema principal active en este enlace de subárea. Este parámetro es aplicable sólo si Solicit SSCP session es yes y Enable Host Initiated Dynamic LU Definition es yes.</p> <p>No es necesario utilizar el mandato add implicit-pool para definir esta agrupación; la especificación del nombre y otros parámetros aquí es suficiente para que se cree la agrupación. Si no entra un nombre de agrupación, se le solicitará la entrada de valores para los parámetros siguientes:</p> <ul style="list-style-type: none"> • Pool class (Consulte la Tabla 42 en la página 221) • LU type (Consulte la Tabla 42 en la página 221) <p>Si lo desea, puede proporcionar el mismo nombre de agrupación para varios enlaces de subárea.</p> <p>La especificación de la información de agrupación hace que las LU iniciadas por el sistema principal que todavía no están configuradas en el direccionador se coloquen en la agrupación especificada. Entonces se les pueden asignar clientes de TN3270 solicitando el nombre de agrupación o correlacionando direcciones IP de cliente o puertos de destino con dicha agrupación.</p> <p>Si no se especifica información de agrupación, estas LU iniciadas por el sistema principal son tratadas como LU explícitas y sólo pueden asignarse a clientes que las soliciten por sus propios nombres de LU.</p>

Tabla 24 (Página 10 de 10). Lista de parámetros de configuración - Estaciones de enlace - Detalle

Información de los parámetros	
Parámetro	Local SAP address
Valores válidos	Cualquier dirección de SAP válida entre X'04' y X'EC'.
Valor por omisión	Valor tomado del puerto
Descripción	Este parámetro especifica la dirección de SAP local.
	Notas:
	<ol style="list-style-type: none"> 1. Esta pregunta sólo se visualiza si hay varias PU definidas en el puerto. 2. Si la dirección de SAP local no es la dirección de SAP local principal del puerto, 3. el nombre del puerto y el nombre del SAP se visualizarán al supervisor y en la salida de la visualización de SNMP.
Parámetro	Send Terminate-Self when TN3270 Client Disconnects
Valores válidos	Yes o No
Valor por omisión	No
Descripción	Este parámetro indica si se enviará una solicitud terminate_self a SSCP cuando el cliente de TN3270 se desconecte. Si se especifica yes, se enviará terminate_self y el sistema principal será responsable de la terminación de la sesión de LU-LU (es decir, la SLU NO enviará una solicitud UNBIND.)
Parámetro	Subnet visit count
Valores válidos	De 1 a 255
Valor por omisión	El valor por omisión se toma del parámetro de nivel de puerto equivalente
Descripción	Este parámetro especifica el valor por omisión del número máximo de subredes que puede atravesar una sesión de varias subredes.
	Nota: Esta pregunta sólo se hace si la función de nodo de frontera está habilitada en este nodo.
Parámetro	Adjacent node subnet affiliation
Valores válidos	<ul style="list-style-type: none"> • 0 (nativa) • 1 (no nativa) • 2 (negociable)
Valor por omisión	El valor por omisión se toma del parámetro de nivel de puerto equivalente
Descripción	Este parámetro especifica si el nodo adyacente está en la subred APPN nativa del nodo o en una subred APPN no nativa. Un valor de 2 instruye al nodo para que negocie en el momento de activación del enlace para determinar si la estación de enlace adyacente es nativa o no.
	Nota: Esta pregunta sólo se hace si la función de nodo de frontera está habilitada en este nodo.

Mandatos de configuración de APPN

<i>Tabla 25 (Página 1 de 5). Lista de parámetros de configuración - Configuración de estación para ATM</i>	
Información de los parámetros	
Parámetro	Virtual Channel Type
Valores válidos	SVC, PVC
Valor por omisión	SVC
Descripción	Este parámetro identifica el tipo de canal ATM como un circuito virtual conmutado (SVC) o un circuito virtual permanente (PVC).
Nota: Los parámetros siguientes son comunes para los SVC y los PVC.	
Parámetro	Destination ATM Address
Valores válidos	Serie hexadecimal de 40 caracteres
Valor por omisión	Ninguno
Descripción	Este parámetro especifica la serie de 20 bytes que forma la dirección ATM de destino completa.
Parámetro	ATM network type
Valores válidos	Campus, Widearea
Valor por omisión	Campus
Descripción	Este parámetro especifica el tipo de red ATM.
Parámetro	Shareable connection network traffic
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro especifica si el tráfico de la red de conexiones puede direccionarse en el ATM VC establecido para este TG.
Parámetro	Shareable other protocol traffic
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro especifica si puede direccionarse otro tráfico de protocolo de nivel superior en el ATM VC establecido para este TG.
Parámetro	LDLC retry count
Valores válidos	De 1 a 255
Valor por omisión	3
Descripción	Este parámetro se usa junto con el período del temporizador LDLC para proporcionar una entrega fiable de XID. La cuenta de reintentos se inicializa cuando un mandato o solicitud se transmite por primera vez sobre un enlace. Si el período del temporizador LDLC se agota antes de recibir una respuesta, se volverá a transmitir el mandato o solicitud, la cuenta de reintentos disminuirá y el período del temporizador LDLC se reiniciará. Si el temporizador agota el tiempo con la cuenta de reintentos en 0, se presupondrá que el enlace no es operativo.

<i>Tabla 25 (Página 2 de 5). Lista de parámetros de configuración - Configuración de estación para ATM</i>	
Información de los parámetros	
Parámetro	LDLC Timer Period
Valores válidos	De 1 a 255 segundos
Valor por omisión	Para ATM: 1 segundo Para IP: 15 segundos
Descripción	Este parámetro especifica el período de tiempo usado con LDLC retry count .
Parámetro	VPI
Valores válidos	De 0 a 255
Valor por omisión	0
Descripción	Este parámetro identifica el VPI del PVC de la interfaz.
Parámetro	VCI
Valores válidos	De 0 a 65535
Valor por omisión	0
Descripción	Este parámetro identifica el VCI del PVC de la interfaz.
Parámetro	Broadband Bearer Class
Valores válidos	Class_A, Class_C, Class_X
Valor por omisión	Class_X
Descripción	Este parámetro especifica la clase de portador solicitada desde la red ATM. Las clases se definen del modo siguiente: Class A (Clase A) Velocidad de bit constante (CBR) con requisitos de tiempo de extremo a extremo Class C (Clase C) Velocidad de bit variable (VBR) sin requisitos de tiempo de extremo a extremo Class X (Clase X) Servicio que permite el tipo de tráfico definido por el usuario y requisitos de tiempo
Parámetro	Best Effort Indicator
Valores válidos	Yes, No
Valor por omisión	No
Descripción	Este parámetro indica si se requiere una garantía completa en este SVC. Si el valor de este parámetro es <i>yes</i> , los VCC asociados a esta interfaz se asignarán basándose en la anchura de banda disponible.
Nota: Los parámetros siguientes son parámetros de tráfico de reenvío.	

Mandatos de configuración de APPN

<i>Tabla 25 (Página 3 de 5). Lista de parámetros de configuración - Configuración de estación para ATM</i>	
Información de los parámetros	
Parámetro	Forward Peak Cell Rate
Valores válidos	85% de la velocidad de línea
Valor por omisión	Capacidad efectiva por omisión del puerto/48
Descripción	Este parámetro indica un límite superior en la velocidad de transmisión de células.
Parámetro	Forward Sustained Cell Rate
Valores válidos	Del 1 al 85% de velocidad de línea
Valor por omisión	Capacidad efectiva por omisión del puerto/48
Descripción	Este parámetro indica un límite superior en la velocidad media de transmisión de células. No puede especificar este parámetro para conexiones de Mejor esfuerzo.
Parámetro	Forward Tagging
Valores válidos	Yes, No
Valor por omisión	Yes
Descripción	Este parámetro indica que las células que no cumplen la especificación de tráfico de prioridad 0 de pérdida de células, pero sí que cumplen la especificación de tráfico de prioridad 1 de dicha pérdida se marcan y pueden entrar en la red ATM. No puede especificar este parámetro para conexiones de Mejor esfuerzo.
Parámetro	QoS
Valores válidos	CLASS_0, CLASS_1, CLASS_2, CLASS_3, CLASS_4, donde
	CLASS_0 Clase sin especificar. La red no especifica ninguna QoS.
	CLASS_1 El rendimiento es comparable al de la línea privada digital actual.
	CLASS_2 Clase destinada al vídeo y audio en paquetes para las aplicaciones multimedia y de videoconferencia.
	CLASS_3 Clase destinada al interfuncionamiento de protocolos orientados a la conexión como, por ejemplo, Frame Relay.
	CLASS_4 Clase destinada al interfuncionamiento de protocolos sin conexión como, por ejemplo, IP.
Valor por omisión	CLASS_0
Descripción	Este parámetro indica qué clase de servicio se proporciona a una conexión virtual ATM. No puede especificar este parámetro para conexiones de Mejor esfuerzo.
Nota: Los parámetros siguientes son parámetros de tráfico hacia atrás.	

<i>Tabla 25 (Página 4 de 5). Lista de parámetros de configuración - Configuración de estación para ATM</i>	
Información de los parámetros	
Parámetro	Backward Peak Cell Rate
Valores válidos	Del 1 al 85% de velocidad de línea
Valor por omisión	Tomado de la definición del puerto
Descripción	Este parámetro indica un límite superior en la velocidad de transmisión de células.
Parámetro	Backward Sustained Cell Rate
Valores válidos	Del 1 al 85% de velocidad de línea
Valor por omisión	Tomado de la definición del puerto
Descripción	Este parámetro indica un límite superior en la velocidad media de transmisión de células. No puede especificar este parámetro para conexiones de Mejor esfuerzo.
Parámetro	Backward Tagging
Valores válidos	Yes, No
Valor por omisión	Yes
Descripción	Este parámetro indica que las células que no cumplen la especificación de tráfico de prioridad 0 de pérdida de células, pero sí que cumplen la especificación de tráfico de prioridad 1 de dicha pérdida se marcan y pueden entrar en la red ATM. No puede especificar este parámetro para conexiones de Mejor esfuerzo.
Parámetro	QoS
Valores válidos	CLASS_0, CLASS_1, CLASS_2, CLASS_3, CLASS_4, donde
	CLASS_0 Clase sin especificar. La red no especifica ninguna QoS.
	CLASS_1 El rendimiento es comparable al de la línea privada digital actual.
	CLASS_2 Clase destinada al vídeo y audio en paquetes para las aplicaciones multimedia y de videoconferencia.
	CLASS_3 Clase destinada al interfuncionamiento de protocolos orientados a la conexión como, por ejemplo, Frame Relay.
	CLASS_4 Clase destinada al interfuncionamiento de protocolos sin conexión como, por ejemplo, IP.
Valor por omisión	CLASS_0
Descripción	Este parámetro indica qué clase de servicio se proporciona a una conexión virtual ATM. No puede especificar este parámetro para conexiones de Mejor esfuerzo.

Mandatos de configuración de APPN

Tabla 25 (Página 5 de 5). Lista de parámetros de configuración - Configuración de estación para ATM

Información de los parámetros	
Parámetro	Callout Anonymously
Valores válidos	Yes, No
Valor por omisión	no
Descripción	Este parámetro indica si APPN pasará la dirección de origen cuando llame.

Tabla 26 (Página 1 de 3). Lista de parámetros de configuración - Modificación de las características de los TG

Información de los parámetros	
Parámetro	Cost per connect time
Valores válidos	De 0 a 255
Valor por omisión	El valor por omisión se toma del parámetro del puerto asociado.
Descripción	Este parámetro expresa el coste relativo de mantener una conexión sobre un TG asociado. Las unidades están definidas por el usuario y normalmente se basan en las tarifas aplicables del recurso de transmisión que se está usando. Los valores asignados deben reflejar el gasto real del mantenimiento de una conexión sobre el TG en relación con el resto de los TG de la red. Un valor de cero significa que las conexiones sobre el TG pueden establecerse sin ningún coste adicional (como en el caso de varios de los recursos no conmutados). Los valores más altos representan costes más altos.
Parámetro	Cost per byte
Valores válidos	De 0 a 255
Valor por omisión	El valor por omisión se toma del parámetro del puerto asociado.
Descripción	Este parámetro expresa el coste relativo de transmitir un byte sobre el TG asociado. Las unidades están definidas por el usuario y el valor asignado debe reflejar los gastos reales de transmisión sobre el TG en relación con el resto de TG de la red. Un valor de cero significa que los bytes pueden transmitirse sobre el TG sin costes adicionales. Los valores más altos representan costes más altos.

Tabla 26 (Página 2 de 3). Lista de parámetros de configuración - Modificación de las características de los TG

Información de los parámetros	
Parámetro	Security
Valores válidos	<ul style="list-style-type: none"> • Nonsecure (no fiable) - el resto (por ejemplo, conectado por satélite o situado en un país no fiable). • Public switched network (red conmutada pública) - fiable en el sentido de que la ruta no se determina previamente. • Underground cable (cable subterráneo) - situado en un país fiable (determinado por el administrador de red). • Secure conduit (Conducto fiable) - sin guardar, (por ejemplo, conducto presurizado). • Guarded conduit (Conducto vigilado) - protegido contra las intervenciones físicas. • Encrypted (Cifrado) - se proporciona un cifrado de nivel de enlace. • Guarded radiation (Radiación vigilada) - conducto vigilado que contiene el medio de transmisión; protegido contra la intervención de radiación y la intervención física.
Valor por omisión	El valor por omisión se toma del parámetro del puerto asociado.
Descripción	Este parámetro indica el nivel de seguridad asociado al TG. Si se necesitan atributos de seguridad que no sean los definidos arquitecturalmente, puede usarse una de las características de TG definidas por el usuario para especificar valores adicionales.
Parámetro	Propagation delay
Valores válidos	<p>Minimum LAN (LAN mínima) – menos de 480 microsegundos</p> <p>Telephone (Teléfono) – entre 0,48 y 49,152 milisegundos</p> <p>Packet switched (Paquete conmutado) - entre 49,152 y 245,76 milisegundos</p> <p>Satellite (Satélite) - superior a 245,76 milisegundos Máximo</p>
Valor por omisión	El valor por omisión se toma del parámetro del puerto asociado.
Descripción	Este parámetro especifica el rango aproximado del período de tiempo que tarda en propagarse una señal desde un extremo del TG hasta el otro.
Parámetro	Effective capacity
Valores válidos	2 dígitos hexadecimales del rango incluido entre X'00' y X'FF'
Valor por omisión	El valor por omisión se toma del parámetro del puerto asociado.
Descripción	<p>Este parámetro especifica la velocidad de transmisión de bits máxima para los enlaces físicos y los lógicos. Observe que la capacidad efectiva de un enlace lógico puede ser inferior a la velocidad de enlace físico.</p> <p>La capacidad efectiva está codificada como representación de un único byte. Los valores X'00' y X'FF' son casos especiales usados para denotar las capacidades mínima y máxima. El rango de codificación es muy amplio; no obstante, sólo se pueden especificar 256 valores del rango.</p>

Tabla 26 (Página 3 de 3). Lista de parámetros de configuración - Modificación de las características de los TG	
Información de los parámetros	
Parámetro	First user-defined TG characteristic
Valores válidos	De 0 a 255
Valor por omisión	El valor por omisión se toma del parámetro del puerto asociado.
Descripción	Este parámetro especifica la primera de tres características adicionales que los usuarios pueden definir para describir los TG de una red.
Parámetro	Second user-defined TG characteristic
Valores válidos	De 0 a 255
Valor por omisión	El valor por omisión se toma del parámetro del puerto asociado.
Descripción	Este parámetro especifica la segunda de tres características adicionales que los usuarios pueden definir para describir los TG de una red.
Parámetro	Third user-defined TG characteristic
Valores válidos	De 0 a 255
Valor por omisión	El valor por omisión se toma del parámetro del puerto asociado.
Descripción	Este parámetro especifica la tercera de tres características adicionales que los usuarios pueden definir para describir los TG de una red.

Tabla 27 (Página 1 de 2). Lista de parámetros de configuración - Modificación del servidor de LU dependientes	
Información de los parámetros	
Parámetro	fully-qualified CP name of primary DLUS
Valores válidos	Una serie con un máximo de 17 caracteres presentados en forma de <i>IDred.nombreCP</i> , donde: <ul style="list-style-type: none"> • <i>IDred</i> es un ID de red de 1 a 8 caracteres • <i>nombreCP</i> es un nombre de punto de control que tiene entre 1 y 8 caracteres <p>Cada nombre debe respetar las normas siguientes:</p> <ul style="list-style-type: none"> • Primer carácter: De la A a la Z • Del segundo al octavo carácter: De la A a la Z, de 0 a 9 <p>Nota: Sigue dándose soporte a nombres de CP plenamente calificados que usan los caracteres especiales @, \$ y # del juego de caracteres A; no obstante, estos caracteres no deben usarse en los nombres de CP nuevos.</p>
Valor por omisión	El valor por omisión especificado en el parámetro del nombre del CP plenamente calificado del servidor de LU dependientes primario.
Descripción	Este parámetro especifica el nombre del CP plenamente calificado del servidor de LU dependientes (DLUS) que se va a usar para las solicitudes de entrada de la PU en sentido directo asociada a esta estación de enlace.

Tabla 27 (Página 2 de 2). Lista de parámetros de configuración - Modificación del servidor de LU dependientes

Información de los parámetros	
Parámetro	fully-qualified CP name for backup DLUS
Valores válidos	<p>Una serie con un máximo de 17 caracteres presentados en forma de <i>IDred.nombreCP</i>, donde:</p> <ul style="list-style-type: none"> • <i>IDred</i> es un ID de red de 1 a 8 caracteres • <i>nombreCP</i> es un nombre de punto de control que tiene entre 1 y 8 caracteres <p>Cada nombre debe respetar las normas siguientes:</p> <ul style="list-style-type: none"> • Primer carácter: De la A a la Z • Del segundo al octavo carácter: De la A a la Z, de 0 a 9 <p>Nota: Sigue dándose soporte a nombres de CP plenamente calificados que usan los caracteres especiales @, \$ y # del juego de caracteres A; no obstante, estos caracteres no deben usarse en los nombres de CP nuevos.</p>
Valor por omisión	El valor especificado en el parámetro del nombre del CP plenamente calificado por omisión del servidor de LU dependientes.
Descripción	Este parámetro especifica el nombre del CP plenamente calificado del servidor de LU dependientes (DLUS) que se va a usar como elemento de seguridad para la PU en sentido directo asociada a esta estación de enlace. Este parámetro permite alterar temporalmente el servidor de seguridad por omisión. No se necesita un elemento de seguridad y el valor NULL indica la ausencia de un servidor de seguridad. Tenga en cuenta que puede especificarse NULL, incluso cuando se ha definido un servidor de seguridad por omisión (borrando el valor por omisión que aparece para este parámetro).

Tabla 28 (Página 1 de 3). Lista de parámetros de configuración - Modificación de las características del LLC

Información de los parámetros	
Parámetro	Remote APPN SAP
Valores válidos	Múltiplos de cuatro del rango hexadecimal incluido entre X'04' y X'EC'.
Valor por omisión	El valor por omisión se toma del parámetro del puerto asociado.
Descripción	Este parámetro especifica la dirección de SAP de destino (DSAP) del nodo de destino al que se enviarán los datos. El valor de la dirección DSAP aparecerá en la trama LLC para identificar la dirección del punto de acceso de los servicios (SAP) asociada a la estación de enlace de APPN del nodo adyacente.
Parámetro	Maximum number of outstanding I-format LPDUs (TW)
Valores válidos	De 1 a 127
Valor por omisión	El valor por omisión se toma del parámetro del puerto asociado.
Descripción	Este parámetro especifica la opción de transmisión de la línea de mandatos que es la cantidad máxima de LPDU de formato I numeradas secuencialmente cuyo recibo puede haber dejado sin acusar, en algún momento, la estación de enlace.

<i>Tabla 28 (Página 2 de 3). Lista de parámetros de configuración - Modificación de las características del LLC</i>	
Información de los parámetros	
Parámetro	Receive window size
Valores válidos	De 1 a 127
Valor por omisión	El valor por omisión se toma del parámetro del puerto asociado.
Descripción	Este parámetro especifica la cantidad máxima de LPDU de formato I numeradas secuencialmente y sin acuse de recibo que puede recibir la estación de enlace de LLC de la estación de enlace remota. RW se notifica en tramas SNA XID y tramas IEEE 802.2 XID. El receptor XID debe establecer el TW efectivo en un valor inferior o igual al del RW recibido a fin de evitar desbordamientos.
Parámetro	Inactivity timer (Ti)
Valores válidos	De 1 a 254 segundos
Valor por omisión	El valor por omisión se toma del parámetro del puerto asociado.
Descripción	Una estación de enlace usa Ti para detectar una condición no operativa en la estación de enlace remota o en el soporte de transmisión. Si no se recibe una LPDU en el intervalo de tiempo especificado por el Ti, se transmitirá una LPDU de mandato de formato S con bit de sondeo para solicitar el estado de la estación de enlace remota. La recuperación se basará en el temporizador de respuesta (T1).
Parámetro	Reply timer (T1)
Valores válidos	De 1 a 254 segundos
Valor por omisión	El valor por omisión se toma del parámetro del puerto asociado.
Descripción	Una estación de enlace usa T1 para detectar un fallo en la recepción de un acuse de recibo necesario o una respuesta de la estación remota de enlace. Cuando T1 se agota, la estación de enlace envía una unidad de datos de protocolo de la capa de enlace (LPDU) de mandato de formato S con el bit de sondeo establecido, para solicitar el estado de la estación de enlace remota o cualquier LPDU de mandato de formato U que no haya recibido respuesta. La duración de T1 debe tener en cuenta cualquier retardo introducido en las capas inferiores.
Parámetro	Maximum number of retransmissions (N2)
Valores válidos	De 1 a 254
Valor por omisión	El valor por omisión se toma del parámetro del puerto asociado.
Descripción	Este parámetro especifica el número máximo de veces que una LPDU se volverá a transmitir después de la expiración del temporizador de respuesta (T1).

Tabla 28 (Página 3 de 3). Lista de parámetros de configuración - Modificación de las características del LLC

Información de los parámetros	
Parámetro	Receive acknowledgment timer (T2)
Valores válidos	De 1 a 254, calculado en décimas de segundo
Valor por omisión	El valor por omisión se toma del parámetro del puerto asociado.
Descripción	Este parámetro puede usarse junto con el contador N3 para reducir el tráfico de acuses de recibo. Una estación de enlace usa T2 para retrasar el envío de un acuse de recibo de una LPDU de formato I recibida. T2 se inicia cuando se recibe una LPDU de formato I y se restablece cuando se envía un acuse de recibo en una LPDU de formato I o formato S. Si T2 expira, la estación de enlace deberá enviar un acuse de recibo tan pronto como sea posible. El valor de T2 debe ser inferior al de T1, para asegurarse de que la estación de enlace remota reciba el acuse de recibo retrasado antes de que expire su T1.
Parámetro	Acknowledgment needed to increment working window
Valores válidos	De 0 a 127 acuses de recibo
Valor por omisión	El valor por omisión se toma del parámetro del puerto asociado.
Descripción	Cuando la ventana de trabajo (Ww) no es igual al tamaño máximo de la ventana de transmisión (Maximum Transmit Window Size - Tw), este parámetro será la cantidad de LPDU de formato I transmitidas cuyo acuse de recibo debe efectuarse antes de poder incrementar la ventana de trabajo (en 1). Cuando se detecta una congestión, por la pérdida de LPDU de formato I, Ww se establece en 1.

Tabla 29 (Página 1 de 2). Lista de parámetros de configuración - Modificación de los valores por omisión de HPR

Información de los parámetros	
Parámetro	Inactivity timer override for HPR (HPR Ti)
Valores válidos	De 1 a 254 segundos
Valor por omisión	El valor por omisión se toma del parámetro del puerto asociado.
Descripción	Este parámetro especifica el temporizador de inactividad de LLC de alteración temporal de HPR (HPR Ti) que se usará cuando HPR tenga soporte de esta estación de enlace. Este parámetro altera temporalmente el valor que se toma del valor por omisión de alteración temporal del temporizador de inactividad para el parámetro HPR. Este parámetro se impone sobre el valor asignado al parámetro del temporizador de inactividad (Ti) de LLC especificado en el parámetro de modificación de las características del control de enlace lógico (LLC) cuando se da soporte a HPR.

<i>Tabla 29 (Página 2 de 2). Lista de parámetros de configuración - Modificación de los valores por omisión de HPR</i>	
Información de los parámetros	
Parámetro	Reply timer override for HPR (HPR T1)
Valores válidos	De 1 a 254 segundos
Valor por omisión	El valor por omisión se toma del parámetro del puerto asociado.
Descripción	<p>Este parámetro especifica el temporizador de respuesta de LLC de alteración temporal de HPR (HPR T1) que se usará cuando HPR tenga soporte de esta estación de enlace. Este parámetro altera temporalmente el valor por omisión tomado del parámetro de alteración temporal del temporizador de respuesta para HPR especificado en los valores por omisión de HPR.</p> <p>Este parámetro se impone sobre el valor asignado al parámetro del temporizador de respuesta (T1) de LLC especificado en el parámetro de modificación de las características del control de enlace lógico (LLC) cuando se da soporte a HPR.</p>
Parámetro	Maximum number retransmission (HPR N2)
Valores válidos	De 1 a 216000
Valor por omisión	El valor por omisión se toma del parámetro del puerto asociado.
Descripción	<p>Este parámetro especifica el número máximo de LLC de alteración temporal de HPR de retransmisiones (HPR N2) que se usará cuando HPR tenga el soporte de esta estación de enlace. Este parámetro altera temporalmente el valor por omisión tomado del parámetro del número máximo de retransmisiones para HPR especificado en los valores por omisión de alteración del HPR LLC.</p> <p>Este parámetro se impone sobre el valor asignado al parámetro del número máximo de LLC de retransmisiones (N2) especificado en el parámetro de modificación de las características del control de enlace lógico (LLC) cuando HPR tiene soporte.</p>
Parámetro	Limited Resource Timer
Valores válidos	De 1 a 216000 segundos
Valor por omisión	El valor por omisión se toma del parámetro del puerto asociado.
Descripción	Este parámetro especifica el valor del temporizador asociado al recurso limitado.

Sintaxis:

add

lu-name

Se le solicitará que entre un nombre de estación para asociarlo con esta LU.

También se le solicitará que entre un valor para el parámetro siguiente. El rango del parámetro se mostrará entre paréntesis (). El valor por omisión del parámetro se mostrará entre corchetes [].

Tabla 30. Lista de parámetros de configuración - Nombre de la LU del nodo final LEN

Información de los parámetros	
Parámetro	fully-qualified LU name
Valores válidos	<p>Nombre de LU plenamente calificado (explícito); nombre de LU genérico (parcialmente explícito; entrada comodín)</p> <p>Una serie con un máximo de 17 caracteres presentados en forma de <i>IDred.nombreLU</i>, donde:</p> <ul style="list-style-type: none"> • <i>IDred</i> es un ID de red de 1 a 8 caracteres • <i>nombreLU</i> es un nombre de punto de control que tiene entre 1 y 8 caracteres <p>Cada nombre debe respetar las normas siguientes:</p> <ul style="list-style-type: none"> • Primer carácter: De la A a la Z • Del segundo al octavo carácter: De la A a la Z, de 0 a 9 <p>Nota: Sigue dándose soporte a nombres de LU plenamente calificados que usan los caracteres especiales @, \$ y # del juego de caracteres A; no obstante, estos caracteres no deben usarse para nombres de LU nuevos.</p> <p>Para reducir el número de nombres de LU plenamente calificados que debe especificar, puede definir un nombre de LU genérico usando el carácter comodín (*) para representar una parte del nombre de LU (<i>nombreLU</i>). También puede definir una entrada comodín usando el carácter comodín como nombre de LU completo.</p>
Valor por omisión	Ninguno
Descripción	<p>Este parámetro especifica los nombres plenamente calificados de las LU asociadas a un nodo final LEN. Los nombres de LU que se especifiquen se registrarán en la base de datos de servicios del directorio del nodo de red. Si no se registra un nombre, el nodo de red no podrá localizar la LU (a menos que dicho nombre sea el mismo que el nombre del CP del nodo final LEN).</p> <p>Debe especificarse un nombre de LU plenamente calificado, formado por un ID de red y el nombre de la LU. El ID de red es el nombre de la red que contiene el nodo final LEN adyacente. El nombre de la LU es el nombre de una unidad lógica a la que se puede acceder a través del nodo final LEN adyacente.</p>

Sintaxis:

add connection-network

Se le solicitará que entre los valores de los parámetros siguientes. El rango del parámetro se mostrará entre paréntesis (). El valor por omisión del parámetro se mostrará entre corchetes [].

<p>Tabla 31 (Página 1 de 3). Lista de parámetros de configuración - Red de conexiones - Detalle</p>	
<p>Información de los parámetros</p>	
<p>Parámetro</p>	<p>Fully-qualified Connection network name (obligatorio para todas las redes de conexiones definidas)</p>
<p>Valores válidos</p>	<p>Una serie de 1 a 8 caracteres:</p> <ul style="list-style-type: none"> • Primer carácter: De la A a la Z • Del segundo al octavo carácter: De la A a la Z, de 0 a 9 <p>Nota: Sigue dándose soporte a una red de conexiones existente a la que este nodo desea pertenecer y cuyo nombre tiene los caracteres especiales @, \$ y # del juego de caracteres A; no obstante, estos caracteres no deben usarse para nombres de red de conexiones nuevos.</p>
<p>Valor por omisión</p>	<p>Ninguno</p>
<p>Descripción</p>	<p>Este parámetro especifica el nombre plenamente calificado de la red de conexiones que se está definiendo en este nodo de red del direccionador. Dado que este nombre se convierte en el nombre del CP del nodo de direccionamiento virtual (VRN), deberá ser único entre todos los nombres de CP y de LU de la red APPN (igual que en el nombre del punto de control local).</p> <p>Todos los nodos que sean miembros de una red de conexiones determinada deben usar el mismo nombre de VRN.</p> <p>El nombre de VRN plenamente calificado (nombre del CP del VRN) tiene el formato:</p> <p><i>IDRed.NombreRedConexión</i> donde <i>IDRed</i> es el identificador de red de este nodo de red del direccionador.</p>
<p>Parámetro</p>	<p>Port type (obligatorio)</p>
<p>Valores válidos</p>	<p>Token-ring (red en anillo), Ethernet, Frame Relay BAN, IP, ATM</p> <p>Nota: Si el port type es IP, no se especificará ningún port name ya que sólo habrá un puerto IP.</p>
<p>Valor por omisión</p>	<p>Ninguno</p>
<p>Descripción</p>	<p>Este parámetro especifica los tipos de puertos que dan conectividad al SATF para la red de conexiones que se está definiendo. Una red de conexiones determinada sólo dará soporte a un tipo de puerto con un conjunto de características.</p>

Tabla 31 (Página 2 de 3). Lista de parámetros de configuración - Red de conexiones - Detalle

Información de los parámetros	
Parámetro	Port name (obligatorio)
Valores válidos	Nombre del puerto en el que se ha habilitado el direccionamiento de APPN. Nota: Si el port type es IP, no se especificará ningún port name ya que sólo habrá un puerto IP.
Valor por omisión	Ninguno
Descripción	Este parámetro especifica el nombre de un puerto que da conectividad con el recurso de transporte de acceso compartido (SATF) a la red de conexiones que se está definiendo. Todos los puertos definidos para una red de conexiones determinada deben ser del mismo tipo y tener las mismas características. Nota: Para un tipo de puerto de IP, los puertos adicionales añadidos a una red de conexiones IP pueden ser cualquiera cuyo uso se haya definido para IP. Debe añadirse como mínimo un puerto adicional al puerto IP para la red de conexiones que vaya a usarse. Dado que el puerto IP es un pseudo puerto que siempre se activa cuando el nodo se inicializa, deben añadirse al CN puertos reales sobre los que IP esté definido (TR, ATM, FR, ...). Cuando como mínimo uno de estos puertos reales esté activo, se presupondrá que el enlace de red de conexiones está activo. Cuando todos estos puertos reales estén inactivos, se presupondrá que el enlace de red de conexiones está inactivo.
Parámetro	Limited Resource Timer
Valores válidos	De 1 a 216000 segundos
Valor por omisión	180
Descripción	Este parámetro especifica el valor del temporizador asociado a un recurso limitado.
Parámetro	DLCI number
Valores válidos	De 16 a 1007
Valor por omisión	Ninguno
Descripción	Este parámetro especifica el número de DLCI usado por el direccionador para conectarse con la red Frame Relay. Cuando el direccionador inicie una conexión con una estación de enlace de la LAN a través de la red de conexiones, usará este número de DLCI para conectarse con la red Frame Relay.

Mandatos de configuración de APPN

<i>Tabla 31 (Página 3 de 3). Lista de parámetros de configuración - Red de conexiones - Detalle</i>	
Información de los parámetros	
Parámetro	BAN destination address (BDA)
Valores válidos	De X'0000 0000 0000' a X'7FFF FFFF FFFF'
Valor por omisión	X'0000 0000 0000'
Descripción	Este parámetro especifica la dirección de destino de la BAN configurada en el nodo que está ejecutando la función BAN. Si está usando el puenteo para conectar la red LAN con la red Frame Relay, especifique X'0000 0000 0000' como valor de este parámetro. En dicho caso, la dirección del MAC indicada a la topología APPN para el TG de la red de conexiones será la dirección BNI MAC codificada en el puerto APPN asociado a esta definición de red de conexiones.

<i>Tabla 32 (Página 1 de 4). Lista de parámetros de configuración - Configuración de la red de conexiones para ATM</i>	
Información de los parámetros	
Parámetro	Port name (obligatorio)
Valores válidos	Nombre del puerto en el que se ha habilitado el direccionamiento de APPN.
Valor por omisión	Ninguno
Descripción	Este parámetro especifica el nombre de un puerto que da conectividad con el recurso de transporte de acceso compartido (SATF) a la red de conexiones que se está definiendo. Todos los puertos definidos para una red de conexiones determinada deben ser del mismo tipo y tener las mismas características.
Parámetro	fully-qualified connection network name
Valores válidos	Una serie de 3 a 17 caracteres con la forma <i>IDred.nombreCN</i> , donde: <ul style="list-style-type: none"> • <i>IDred</i> es un ID de red de 1 a 8 caracteres • <i>nombreCN</i> es el nombre de una red de conexiones de 1 a 8 caracteres Cada nombre debe respetar las normas siguientes: <ul style="list-style-type: none"> • Primer carácter: De la A a la Z • Del segundo al octavo carácter: De la A a la Z, de 0 a 9
Valor por omisión	Ninguno
Descripción	Este parámetro especifica el nombre de CN plenamente calificado en el que este TG está definido.
Parámetro	Connection network TG number
Valores válidos	De 1 a 239
Valor por omisión	Ninguno
Descripción	Este parámetro especifica de forma única el número de TG identificando esta conexión del puerto local a la CN. El par compuesto por el nombre de CN y el número de TG debe ser único.

<i>Tabla 32 (Página 2 de 4). Lista de parámetros de configuración - Configuración de la red de conexiones para ATM</i>	
Información de los parámetros	
Parámetro	Limited Resource
Valores válidos	Yes o No
Valor por omisión	Yes
Descripción	Este parámetro indica si hay que desactivar este TG cuando no se usa en el tráfico de sesión.
Parámetro	Limited Resource Timer
Valores válidos	De 1 a 2 160 000 segundos
Valor por omisión	180 segundos
Descripción	Este parámetro indica el límite de tiempo tras el cual debe desactivarse este CN TG cuando no lo usa una sesión de tráfico.
Parámetro	LDLC retry count
Valores válidos	De 1 a 255
Valor por omisión	3
Descripción	Este parámetro se usa junto con el período del temporizador LDLC para proporcionar una entrega fiable de XID. La cuenta de reintentos se inicializa cuando un mandato o solicitud se transmite por primera vez sobre un enlace. Si el período del temporizador LDLC se agota antes de recibir una respuesta, se volverá a transmitir el mandato o solicitud, la cuenta de reintentos disminuirá y el período del temporizador LDLC se reiniciará. Si el temporizador agota el tiempo con la cuenta de reintentos en 0, se presupondrá que el enlace no es operativo.
Parámetro	LDLC Timer Period
Valores válidos	De 1 a 255 segundos
Valor por omisión	Para ATM: 1 segundo Para IP: 15 segundos
Descripción	Este parámetro especifica el período de tiempo usado con LDLC retry count .

<i>Tabla 32 (Página 3 de 4). Lista de parámetros de configuración - Configuración de la red de conexiones para ATM</i>	
Información de los parámetros	
Parámetro	Broadband Bearer Class
Valores válidos	Class_A, Class_C, o Class_X
Valor por omisión	Class_X
Descripción	Este parámetro especifica la clase de portador solicitada desde la red ATM. Las clases se definen del modo siguiente: Class A (Clase A) Velocidad de bit constante (CBR) con requisitos de tiempo de extremo a extremo Class C (Clase C) Velocidad de bit variable (VBR) sin requisitos de tiempo de extremo a extremo Class X (Clase X) Servicio que permite el tipo de tráfico definido por el usuario y requisitos de tiempo
Parámetro	Shareable Regular Network traffic
Valores válidos	Yes o No
Valor por omisión	Yes, si se trata de un CN de mejor esfuerzo. De lo contrario, no.
Descripción	Este parámetro especifica si el tráfico de este TG de la red de conexiones puede direccionarse en un ATM VC establecido para un TG regular u otro CN TG.
Parámetro	Shareable other protocol traffic
Valores válidos	Yes o No
Valor por omisión	No
Descripción	Este parámetro especifica si el ATM VC establecido para este CN TG puede compartirse con otros protocolos de nivel superior del direccionador.
Nota: Los parámetros siguientes son parámetros de tráfico de reenvío.	
Parámetro	Forward Peak Cell Rate
Valores válidos	Del 1 al 85% de velocidad de línea
Valor por omisión	Tomado de la definición del puerto
Descripción	Este parámetro indica un límite superior en la velocidad de transmisión de células.
Parámetro	Forward Sustained Cell Rate
Valores válidos	Del 1 al 85% de velocidad de línea
Valor por omisión	Tomado de la definición del puerto
Descripción	Este parámetro indica un límite superior en la velocidad media de transmisión de células.

Tabla 32 (Página 4 de 4). Lista de parámetros de configuración - Configuración de la red de conexiones para ATM

Información de los parámetros	
Parámetro	Forward Tagging
Valores válidos	Yes o No
Valor por omisión	Yes
Descripción	Este parámetro indica que las células que no cumplen la especificación de tráfico de prioridad 0 de pérdida de células, pero sí que cumplen la especificación de tráfico de prioridad 1 de dicha pérdida se marcan y pueden entrar en la red ATM.
Parámetro	QoS
Valores válidos	CLASS_0, CLASS_1, CLASS_2, CLASS_3, CLASS_4, donde
	CLASS_0 Clase sin especificar. La red no especifica ninguna QoS.
	CLASS_1 El rendimiento es comparable al de la línea privada digital actual.
	CLASS_2 Clase destinada al vídeo y audio en paquetes para las aplicaciones multimedia y de videoconferencia.
	CLASS_3 Clase destinada al interfuncionamiento de protocolos orientados a la conexión como, por ejemplo, Frame Relay.
	CLASS_4 Clase destinada al interfuncionamiento de protocolos sin conexión como, por ejemplo, IP.
Valor por omisión	CLASS_3
Descripción	Este parámetro indica qué clase de servicio se proporciona a una conexión virtual ATM.

Tabla 33 (Página 1 de 3). Lista de parámetros de configuración - Características de los TG (red de conexiones)

Información de los parámetros	
Parámetro	Cost per connect time
Valores válidos	De 0 a 255
Valor por omisión	0
Descripción	Este parámetro expresa el coste relativo de mantener una conexión sobre un TG asociado. Las unidades están definidas por el usuario y normalmente se basan en las tarifas aplicables del recurso de transmisión que se está usando. Los valores asignados deben reflejar el gasto real del mantenimiento de una conexión sobre el TG en relación con el resto de los TG de la red. Un valor de cero significa que las conexiones sobre el TG pueden establecerse sin ningún coste adicional (como en el caso de varios de los recursos no conmutados). Los valores más altos representan costes más altos.

<i>Tabla 33 (Página 2 de 3). Lista de parámetros de configuración - Características de los TG (red de conexiones)</i>	
Información de los parámetros	
Parámetro	Cost per byte
Valores válidos	De 0 a 255
Valor por omisión	0
Descripción	Este parámetro expresa el coste relativo de transmitir un byte sobre el TG asociado. Las unidades están definidas por el usuario y el valor asignado debe reflejar los gastos reales de transmisión sobre el TG en relación con el resto de TG de la red. Un valor de cero significa que los bytes pueden transmitirse sobre el TG sin costes adicionales. Los valores más altos representan costes más altos.
Parámetro	Security
Valores válidos	<p>Nonsecure (no fiable) - el resto (por ejemplo, conectado por satélite o situado en un país no fiable).</p> <p>Public switched network (red conmutada pública) - fiable en el sentido de que la ruta no se determina previamente.</p> <p>Underground cable (cable subterráneo) - situado en un país fiable (determinado por el administrador de red).</p> <p>Secure conduit (Conducto fiable) - sin guardar, (por ejemplo, conducto presurizado).</p> <p>Guarded conduit (Conducto vigilado) - protegido contra las intervenciones físicas.</p> <p>Encrypted (Cifrado) - se proporciona un cifrado de nivel de enlace.</p> <p>Guarded radiation (Radiación vigilada) - conducto vigilado que contiene el medio de transmisión; protegido contra la intervención de radiación y la intervención física.</p>
Valor por omisión	Nonsecure (no fiable)
Descripción	Este parámetro indica el nivel de seguridad asociado al TG. Si se necesitan atributos de seguridad que no sean los definidos arquitecturalmente, puede usarse una de las características de TG definidas por el usuario para especificar valores adicionales.
Parámetro	Propagation delay
Valores válidos	<ul style="list-style-type: none"> • Minimum LAN (LAN mínima) – menos de 480 microsegundos • Telephone (Teléfono) – entre 0,48 y 49,152 milisegundos • Packet switched (Paquete conmutado) – entre 49,152 y 245,76 milisegundos • Satellite (Satélite) – superior a 245,76 milisegundos Máximo
Valor por omisión	LAN
Descripción	Este parámetro especifica el rango aproximado del período de tiempo que tarda en propagarse una señal desde un extremo del TG hasta el otro.

Tabla 33 (Página 3 de 3). Lista de parámetros de configuración - Características de los TG (red de conexiones)

Información de los parámetros	
Parámetro	Effective capacity
Valores válidos	2 dígitos hexadecimales del rango incluido entre X'00' y X'FF'
Valor por omisión	X'75'
Descripción	<p>Este parámetro especifica la velocidad de transmisión de bits máxima efectiva para este TG de red de conexiones. La capacidad efectiva especifica la velocidad efectiva máxima para los enlaces físicos y los lógicos.</p> <p>La capacidad efectiva está codificada como representación de un único byte. Los valores X'00' y X'FF' son casos especiales usados para denotar las capacidades mínima y máxima. El rango de codificación es muy amplio; no obstante, sólo se pueden especificar 256 valores del rango.</p>
Parámetro	First user-defined characteristic
Valores válidos	De 0 a 255
Valor por omisión	128
Descripción	Este parámetro especifica la primera de tres características adicionales que los usuarios pueden definir para describir los TG de la red. El valor por omisión de 128 permite definir un subconjunto de TG como más o menos deseable que el resto sin tener que definir valores para todos los TG.
Parámetro	Second user-defined characteristic
Valores válidos	De 0 a 255
Valor por omisión	128
Descripción	Este parámetro especifica la segunda de tres características adicionales que los usuarios pueden definir para describir los TG de la red. El valor por omisión de 128 permite definir un subconjunto de TG como más o menos deseable que el resto sin tener que definir valores para todos los TG.
Parámetro	Third user-defined characteristic
Valores válidos	De 0 a 255
Valor por omisión	128
Descripción	Este parámetro especifica la tercera de tres características adicionales que los usuarios pueden definir para describir los TG de la red. El valor por omisión de 128 permite definir un subconjunto de TG como más o menos deseable que el resto sin tener que definir valores para todos los TG.

Sintaxis:

add mode

Se le solicitará que entre los valores de los parámetros siguientes. El rango del parámetro se mostrará entre paréntesis (). El valor por omisión del parámetro se mostrará entre corchetes [].

Tabla 34. Lista de parámetros de configuración - APPN COS - Correlación del nombre de modalidad con el nombre de COS - Detalle

Información de los parámetros	
Parámetro	Mode name (obligatorio)
Valores válidos	Una serie de 1 a 8 caracteres: <ul style="list-style-type: none"> • Primer carácter: De la A a la Z • Del segundo al octavo carácter: De la A a la Z, de 0 a 9
Nota:	Se sigue dando soporte a un nombre de modalidad existente para una red existente a la cual este nodo de red del direccionador va a pertenecer y que usa los caracteres especiales @, \$ y # del juego de caracteres A; no obstante, estos caracteres no deben usarse en los nombres de modalidad nuevos.
Valor por omisión	Ninguno
Descripción	Este parámetro especifica el nombre de modalidad para la correlación de nombre de modalidad con nombre de COS que se está definiendo. Consulte "Opciones de CoS" en la página 39 para obtener información adicional sobre la correlación de nombre de modalidad con COS.
Parámetro	COS name (obligatorio)
Valores válidos	El nombre de una definición de COS establecida previamente, seleccionado en la lista de nombres de COS definida para este nodo de red del direccionador.
Valor por omisión	Ninguno
Descripción	Este parámetro especifica el nombre de COS que se asociará al nombre de modalidad que se está definiendo para esta correlación de nombre de modalidad con nombre de COS.
Parámetro	Session-level pacing Command Line option size
Valores válidos	De 1 a 63
Valor por omisión	7
Descripción	Este parámetro especifica el tamaño de la opción de la línea de mandatos del ritmo del nivel de sesión. Este parámetro tendrá definiciones diferentes según el tipo de ritmo usado: <ul style="list-style-type: none"> • Para el ritmo de nivel de sesión fijo: <ul style="list-style-type: none"> – El parámetro del tamaño de la opción de la línea de mandatos del ritmo del nivel de sesión especificará la opción de la línea de mandatos del ritmo de recepción de este nodo. – El valor de este parámetro es la opción sugerida por la línea de mandatos de recepción para el nodo adyacente. • Para el ritmo de nivel de sesión adaptable: <ul style="list-style-type: none"> – El parámetro del tamaño de la opción de la línea de mandatos del ritmo del nivel de sesión especificará un parámetro de ajuste que se usará como tamaño mínimo para los mensajes de ritmo aislados enviados por los nodos adyacentes.

Syntax:

add

additional-port-to-connection-network

Se le solicitará que entre los valores de los parámetros siguientes. El rango del parámetro se mostrará entre paréntesis (). El valor por omisión del parámetro se mostrará entre corchetes [].

Nota: Puede tener un máximo de 5 puertos por definición de red de conexiones.

Tabla 35. Lista de parámetros de configuración - Puerto adicional APPN a red de conexiones

Información de los parámetros	
Parámetro	Connection network name (fully-qualified) (obligatorio para todas las redes de conexiones definidas)
Valores válidos	<p>Una serie de 1 a 8 caracteres:</p> <ul style="list-style-type: none"> • Primer carácter: De la A a la Z • Del segundo al octavo carácter: De la A a la Z, de 0 a 9 <p>Nota: Sigue dándose soporte a una red de conexiones existente a la que este nodo desea pertenecer y cuyo nombre tiene los caracteres especiales @, \$ y # del juego de caracteres A; no obstante, estos caracteres no deben usarse para nombres de red de conexiones nuevos.</p>
Valor por omisión	Ninguno
Descripción	<p>Este parámetro especifica el nombre de la red de conexiones que se está definiendo en este nodo de red del direccionador. Dado que este nombre se convierte en el nombre del CP del nodo de direccionamiento virtual (VRN), deberá ser único entre todos los nombres de CP y de LU de la red APPN (igual que en el nombre del punto de control local).</p> <p>Todos los nodos que sean miembros de una red de conexiones determinada deben usar el mismo nombre de VRN.</p> <p>El nombre de VRN plenamente calificado (nombre del CP del VRN) tiene el formato:</p> <p><i>IDRed.NombreRedConexión</i> donde <i>IDRed</i> es el identificador de red de este nodo de red del direccionador.</p>
Parámetro	Port name
Valores válidos	<p>Un nombre único no calificado que genera automáticamente la línea de mandatos.</p> <p>El nombre estará formado por:</p> <ul style="list-style-type: none"> • TR (red en anillo) • EN (Ethernet)
Valor por omisión	Nombre no calificado generado por la línea de mandatos.
Descripción	<p>Este parámetro especifica el nombre que representa este puerto.</p> <p>Cuando la red de conexiones a la que se está añadiendo el puerto es IP, sólo se podrán añadir al IP CN los puertos para los que se ha definido que IP tenga una interfaz. Debe añadirse al IP CN, como mínimo, un puerto real que tenga definido IP para que pueda activarse y usarse el CN.</p>

Sintaxis:

Mandatos de configuración de APPN

add

focal_point

Se le solicitará que entre los valores de los parámetros siguientes. El rango del parámetro se mostrará entre paréntesis (). El valor por omisión del parámetro se mostrará entre corchetes [].

Tabla 36. Lista de parámetros de configuración - Punto focal implícito de APPN

Información de los parámetros	
Parámetro	focal point
Valores válidos	Un nombre de CP plenamente calificado
Valor por omisión	Espacios en blanco
Descripción	Este parámetro especifica el nombre de CP plenamente calificado que representa este punto focal. El primer punto focal que se añade es el punto focal implícito primario. Pueden añadirse hasta 8 puntos focales implícitos de seguridad adicionales invocando varias veces Add punto_focal . Si se saca el punto focal implícito primario de la lista de puntos focales con Delete focal_point , el primer punto focal implícito de seguridad, si existe, se convertirá en el punto focal implícito primario.

Sintaxis:

add

local-pu

Se le solicitará que entre los valores de los parámetros siguientes. El rango del parámetro se mostrará entre paréntesis (). El valor por omisión del parámetro se mostrará entre corchetes [].

Tabla 37 (Página 1 de 3). Lista de parámetros de configuración - PU local de APPN

Información de los parámetros	
Parámetro	Station name
Valores válidos	Una serie de 1 a 8 caracteres: <ul style="list-style-type: none"> • Primer carácter: De la A a la Z • Del segundo al octavo carácter: De la A a la Z, de 0 a 9
Valor por omisión	Ninguno
Descripción	Este parámetro especifica el nombre que representa el enlace entre el DLUR y la PU.
Parámetro	Primary DLUS name
Valores válidos	Una serie de 1 a 8 caracteres: <ul style="list-style-type: none"> • Primer carácter: De la A a la Z • Del segundo al octavo carácter: De la A a la Z, de 0 a 9
Valor por omisión	Ninguno
Descripción	Este parámetro especifica el nombre que se usará para alterar temporalmente el DLUS primario configurado para este nodo.

<i>Tabla 37 (Página 2 de 3). Lista de parámetros de configuración - PU local de APPN</i>	
Información de los parámetros	
Parámetro	Secondary DLUS name
Valores válidos	Una serie de 1 a 8 caracteres: <ul style="list-style-type: none"> • Primer carácter: De la A a la Z • Del segundo al octavo carácter: De la A a la Z, de 0 a 9
Valor por omisión	Ninguno
Descripción	Este parámetro especifica el nombre que se usará para alterar temporalmente el DLUS secundario configurado para este nodo.
Parámetro	Autoactivate
Valores válidos	Yes o No
Valor por omisión	Yes
Descripción	Este parámetro especifica si se activa este enlace al arrancar. <p>Nota: Si se va a usar el enlace local para una DDDLPU, deberá especificar <i>yes</i> a esta pregunta.</p> <p>Si el enlace local no se establece en activación automática, el primer intento de usar la pu local (es decir, el primer intento de establecer una sesión TN3270) fallará ya que el enlace todavía no estará activado. Aunque este intento falle, hará que el enlace se active y dicho enlace estará disponible en el intento siguiente. Dado que el enlace se activa cuando se establece la sesión de SSCP-PU y esto es cuando el enlace se identifica como enlace DDDLPU. No puede establecerse ninguna sesión DDDLPU hasta identificar el enlace como enlace DDDLPU.</p>
Parámetro	Enable Host Initiated Dynamic LU Definition
Valores válidos	Yes o No
Valor por omisión	No
Descripción	Este parámetro indica si las LU dependientes se crearán dinámicamente (en oposición a tener que configurarlas). Si se especifica <i>yes</i> , las LU se definirán para esta PU a medida que se reciban solicitudes ACTLU (con CV0E). No es necesario configurar las LU para el servidor de TN3270E.

Tabla 37 (Página 3 de 3). Lista de parámetros de configuración - PU local de APPN	
Información de los parámetros	
Parámetro	Pool Name for Host-initiated Dynamic LUs
Valores válidos	Una serie de 1 a 8 caracteres: <ul style="list-style-type: none"> • Primer carácter: De la A a la Z, \$, #, @, ó < • Del segundo al octavo carácter: De la A a la Z, de 0 a 9, \$, #, @, >, ó <
Valor por omisión	Ninguno
Descripción	<p>Este parámetro especifica el nombre de una agrupación que se creará para contener las LU que el sistema principal active en esta PU local. Este parámetro es aplicable sólo si Enable Host Initiated Dynamic LU Definition es <i>yes</i>.</p> <p>No es necesario utilizar el mandato add implicit-pool para definir esta agrupación; la especificación del nombre y otros parámetros aquí es suficiente para que se cree la agrupación.</p> <p>Si no entra un nombre de agrupación, se le solicitará la entrada de valores para los parámetros siguientes:</p> <ul style="list-style-type: none"> • Pool class (Consulte la Tabla 42 en la página 221) • LU type (Consulte la Tabla 42 en la página 221) <p>Si lo desea, puede proporcionar el mismo nombre de agrupación para varias PU locales.</p> <p>La especificación de la información de agrupación hace que las LU iniciadas por el sistema principal que todavía no están configuradas en el direccionador se coloquen en la agrupación especificada. Entonces se les pueden asignar clientes de TN3270 solicitando el nombre de agrupación o correlacionando direcciones IP de cliente o puertos de destino con dicha agrupación.</p> <p>Si no se especifica información de agrupación, estas LU iniciadas por el sistema principal son tratadas como LU explícitas y sólo pueden asignarse a clientes que las soliciten por sus propios nombres de LU.</p>
Parámetro	Send Terminate-Self when TN3270 Client Disconnects
Valores válidos	Yes o No
Valor por omisión	No
Descripción	Este parámetro indica si se enviará una solicitud terminate_self a SSCP cuando el cliente de TN3270 se desconecte. Si se especifica <i>yes</i> , se enviará terminate_self y el sistema principal será responsable de la terminación de la sesión de LU-LU (es decir, la SLU NO enviará una solicitud UNBIND.)

Sintaxis:

add routing_list

Nota: Estas preguntas sólo se hacen si ha configurado el nodo como nodo de frontera.

Las listas de direccionamientos no tienen soporte en los modelos 2210 12x.

Existe un cierto número de teclas de método abreviado de edición disponibles para acelerar la modificación de datos existentes en una lista de direccionamientos configurada previamente. Estas teclas pueden utilizarse cuando se le soliciten las LU de destino y los CP de direccionamiento.

- Si pulsa **Intro** se mantendrá el nombre que se visualiza actualmente.
- Si pulsa la **Barra espaciadora** seguida de **Intro** se suprimirá el nombre visualizado actualmente.
- Si entra datos de caracteres y luego pulsa **Intro**, se sustituirá el nombre que se visualiza actualmente por los datos de caracteres nuevos.
- Si entra **9** y a continuación pulsa **Intro**, saltará al final de la lista donde se pueden añadir nombres nuevos.
- Al final de una lista, si pulsa **Intro** se completará la lista.

Tabla 38 (Página 1 de 4). Lista de parámetros de configuración - Configuración de la lista de direccionamientos

Información de los parámetros	
Parámetro	Routing list name
Valores válidos	Serie de caracteres que puede tener un máximo de 20 caracteres sin espacios en blanco intercalados. La mezcla de mayúsculas y minúsculas y de caracteres especiales está permitida.
Valor por omisión	Espacio en blanco
Descripción	Este parámetro identifica una lista de direccionamientos para que el código de configuración la modifique, liste o suprima. El código operativo no la usa. Puede configurarse un máximo de 255 listas de direccionamientos según la disponibilidad de la memoria de configuración. Se respetan las mayúsculas y minúsculas.
Parámetro	Subnet visit count
Valores válidos	De 1 a 255
Valor por omisión	El valor por omisión se toma del parámetro de nivel de nodo correspondiente
Descripción	Este parámetro especifica cuántas redes debe atravesar un procedimiento de búsqueda de localización.

<i>Tabla 38 (Página 2 de 4). Lista de parámetros de configuración - Configuración de la lista de direccionamientos</i>	
Información de los parámetros	
Parámetro	Dynamic routing list updates
Valores válidos	0 (ninguna) 1 (completa) 2 (limitada)
Valor por omisión	El valor por omisión se toma del parámetro de nivel de nodo correspondiente
Descripción	Este parámetro controla si puede añadirse automáticamente entradas a la lista de direccionamientos de la subred temporal del nodo. Puede establecerse en los mismos valores que el parámetro de nivel de nodo análogo. Si se habilita esta función las entradas añadidas automáticamente sólo se añadirán a la copia temporal de la lista de direccionamientos.
Parámetro	Enable routing list optimization
Valores válidos	Yes o No
Valor por omisión	Yes
Descripción	Indica si el nodo tiene permiso para reordenar la lista de direccionamientos de la subred para que las entradas que tengan más posibilidades de tener éxito aparezcan en primer lugar. Este reordenamiento se produce en la copia temporal interna de la lista de direccionamientos.

Tabla 38 (Página 3 de 4). Lista de parámetros de configuración - Configuración de la lista de direccionamientos

Información de los parámetros	
Parámetro	Destination LU found via this list
Valores válidos	<p>Nombre de LU plenamente calificado con caracteres comodín finales opcionales. Los caracteres legales para un nombre de LU son: A-Z, @, \$, #, 0-9.</p> <p>El primer carácter de la parte NETID y de la parte del nombre de LU debe ser no numérico.</p> <p>Cualquiera de los nombres de FQ LU puede terminar con un carácter comodín "*" para designar el rango de LU. Por ejemplo,</p> <ul style="list-style-type: none"> • * • NETI* • NETI.LUA*
Valor por omisión	Espacio en blanco
Descripción	<p>Este parámetro especifica una lista de LU de destino que pueden encontrarse a través de esta lista de direccionamientos.</p> <p>Esta pregunta se repetirá hasta que termine con una entrada nula.</p> <p>Notas:</p> <ol style="list-style-type: none"> 1. Sólo una única entrada de todas las listas de direccionamientos puede tener un "*" autónomo. Este coincidirá con todas las LU y la lista de direccionamientos que lo contenga será la lista de direccionamientos por omisión. 2. Todos los métodos abreviados de edición descritos al principio de esta tabla están disponibles para acelerar la modificación de una lista de uno o varios CP de direccionamiento configurada anteriormente. 3. No debe duplicarse ningún nombre de LU determinado en otra lista de direccionamientos. 4. El número máximo de nombres de LU que puede especificarse: <ul style="list-style-type: none"> • 2210 12x - sin soporte • 2210 14x o 24x - 98

Tabla 38 (Página 4 de 4). Lista de parámetros de configuración - Configuración de la lista de direccionamientos

Información de los parámetros	
Parámetro	Routing CP and optional subnet visit count
Valores válidos	<p>Un nombre de CP plenamente calificado formado por un rango incluido entre 1 y 17 caracteres seguido de una cuenta numérica de las visitas a la subred opcional. Los caracteres legales para el nombre de CP son: A-Z, @, \$, #, 0-9</p> <p>El primer carácter de la parte NETID y de la parte del nombre del CP debe ser no numérico. El rango de la cuenta de visitas a la subred opcional está entre 1 y 255 y debe separarse del nombre de CP plenamente calificado por uno o varios espacios.</p>
Valor por omisión	En blanco para un nombre de CP plenamente calificado y establecimiento del nivel de nodo para la cuenta de visitas a la subred.
Descripción	<p>Este parámetro especifica una lista de uno o varios nombres de CP plenamente calificados que pueden saber cómo llegar a una o varias LU de destino configuradas previamente.</p> <p>En cualquier lista de direccionamientos pueden usarse una vez cada una de las palabras clave especiales siguientes:</p> <ul style="list-style-type: none"> • "*" - equivale a especificar todos los BN nativos, todos los BN no nativos adyacentes y todos los NN no nativos adyacentes. • "**SELF" - equivale a especificar el nombre de CP plenamente calificado del nodo local • "**EBNS" - equivale a especificar todos los BN nativos <p>Esta pregunta se repetirá hasta que termine con una entrada nula.</p> <p>Notas:</p> <ol style="list-style-type: none"> 1. Todos los métodos abreviados descritos al principio de esta tabla están disponibles para acelerar la modificación de una lista de CP de direccionamientos configurada previamente. 2. Si configura "**SELF" como nombre de CP, no podrá configurar el nombre de CP del nodo local. 3. Cualquier lista de direccionamientos determinada puede tener el número máximo de nombres de CP y palabras clave siguiente: <ul style="list-style-type: none"> • 2210 12x - sin soporte • 2210 14x o 24x - 96 4. En todas las listas de direccionamientos no puede exceder el número de nombres de CP y palabras clave diferentes siguiente: <ul style="list-style-type: none"> • 2210 12x - sin soporte • 2210 14x o 24x - 96 5. Cualquier nombre de CP o palabra clave determinado no puede aparecer en más de 255 listas de direccionamientos.

Sintaxis:

add cos_mapping_table

Nota: Estas preguntas sólo se hacen si ha configurado el nodo como nodo de frontera (Border Node).

Las tablas de correlaciones de COS no tienen soporte en los modelos 2210 12x.

Las teclas de método abreviado de edición especificadas al principio de la tabla de listas de direccionamiento también son válidas en este caso. Úselas para acelerar la modificación de los nombres de CP no nativos y los pares de nombres COS.

Tabla 39 (Página 1 de 2). Lista de parámetros de configuración - Configuración de la tabla de correlaciones de COS

Información de los parámetros	
Parámetro	COS mapping table name
Valores válidos	Serie de caracteres que puede tener un máximo de 20 caracteres sin espacios en blanco intercalados. La mezcla de mayúsculas y minúsculas y de caracteres especiales está permitida.
Valor por omisión	Espacio en blanco
Descripción	Este parámetro identifica una tabla de correlaciones de COS. Le permite identificar la tabla para que el software de configuración la modifique, liste o suprima. El software operativo no la usa. Puede configurarse un máximo de 255 tablas de correlaciones COS según la disponibilidad de la memoria de configuración. Se respetan las mayúsculas y minúsculas.
Parámetro	Non-native NETID or CP name
Valores válidos	Un nombre de CP plenamente calificado con caracteres comodín finales opcionales. Los caracteres legales para el nombre de CP son: A-Z, @, \$, #, 0-9 El primer carácter de la parte NETID y de la parte del nombre del CP debe ser no numérico. Cualquiera de los nombres de CP plenamente calificados puede terminar con un carácter comodín "*" para designar el rango de CP. Por ejemplo: <ul style="list-style-type: none"> • * • NET1* • NET1.LUA*
Valor por omisión	Espacio en blanco
Descripción	Este parámetro especifica una lista de una o varias redes no nativas en las que se aplica esta tabla de correlaciones. Esta pregunta se repetirá hasta que termine con una entrada nula.
	Notas:
	<ol style="list-style-type: none"> 1. Sólo una única entrada de todas las listas de direccionamientos puede tener un "*" autónomo. Este coincidirá con todas las redes no nativas y será conocido como la lista de direccionamientos por omisión. 2. No debe duplicarse ningún nombre de CP determinado en otra tabla de correlaciones de COS. 3. El número máximo de CP que puede especificarse: <ul style="list-style-type: none"> • 2210 12x - sin soporte • 2210 14x o 24x - 98

Tabla 39 (Página 2 de 2). Lista de parámetros de configuración - Configuración de la tabla de correlaciones de COS

Información de los parámetros	
Parámetro	Native and non-native COS-name pair
Valores válidos	<p>Un par de nombres de COS separados por un espacio en blanco. Los caracteres legales son: A-Z, @, \$, #, 0-9</p> <p>El primer carácter de cada nombre debe ser no numérico.</p>
Valor por omisión	Espacio en blanco
Descripción	<p>Este parámetro identifica un par de nombres de COS. Un nombre de COS nativo va seguido del nombre de COS no nativo correspondiente.</p> <p>En cualquier tabla de correlaciones de COS, uno de los pares de nombres de COS puede especificar el nombre del COS no nativo como “*”. Esto sirve para designar la entrada por omisión que se usará para todos los nombres de COS no nativos que no coincidan explícitamente con otra entrada de la tabla.</p> <p>Un par de nombres de COS no puede coincidir exactamente con otro par de nombres de COS en una tabla determinada. No obstante, puede usarse un nombre de COS nativo determinado en varias entradas y también es adecuado que un nombre de COS no nativo determinado se use en varias entradas. El software operativo usará la primera entrada que encuentre.</p> <p>Esta pregunta se repetirá hasta que termine con una entrada nula.</p> <p>Notas:</p> <ol style="list-style-type: none"> 1. Los nombres nativo y no nativo no pueden ser idénticos. Sólo deben especificarse los nombres de COS que deban cambiarse. 2. Un nombre de COS nativo o no nativo determinado puede aparecer en varias entradas, pero no puede haber dos pares de nombres de COS idénticos. 3. Cuando haya varios nombres de COS nativos que se correlacionen con el mismo nombre de COS no nativo, el nodo de frontera usará la primera de estas correlaciones cuando necesite efectuar una correlación de no nativo a nativo. Asimismo, cuando haya varios nombres de COS no nativos que se correlacionen con un nombre de COS nativo común, el nodo de frontera usará la primera de estas correlaciones cuando necesite efectuar una correlación de nativo a no nativo. 4. Cualquier tabla de correlaciones de COS determinada puede tener el número máximo de pares de nombres de COS siguiente: <ul style="list-style-type: none"> • 2210 12x - sin soporte • 2210 14x o 24x - 46 5. En todas las tablas de correlaciones de COS, no puede usar más del número de nombres de COS nativos siguiente: <ul style="list-style-type: none"> • 2210 12x - sin soporte • 2210 14x o 24x - 96 <p>Los nombres de COS no nativos no tienen un límite análogo.</p> 6. Ningún nombre de COS nativo puede aparecer más de 255 veces en todas las listas de direccionamientos en general.

Delete

Use el mandato **delete** para suprimir:

Sintaxis:

delete port *nombre-puerto*
link *nombre_estación_enlace*
lu-name *nombre_lu*
connection-network *nombre-red-conexión*
additional-port-to-connection-network *nombre-puerto-cn*
mode *nombre*
focal_point *nombre-punto-focal*
local-pu
routing_list *nombre lista direccionamientos*
cos_mapping_table *nombre tabla correlación*

List

Use el mandato **list** para hacer una lista de:

Sintaxis:

list all
node
traces
management
hpr
dlur
port (*nombre puerto*)
link station (*nombre estación enlace*)
lu name *nombre lu*
mode name *nombre modalidad*
connection network *nombre red conexión*
focal_point
routing_list *nombre lista direccionamientos*
cos_mapping_table *nombre tabla correlación*

Activate_new_config

Use el mandato **activate_new_config** para leer la configuración en la memoria no volátil.

Sintaxis:

activate_new_config

TN3270E

Tabla 40. Resumen de los mandatos de configuración de TN3270E

Mandato	Función	Consulte página:
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte la sección "Cómo obtener ayuda" en la página xxix.	
Set	tn3270e	218
Add	Añade o actualiza los elementos siguientes:	
	implicit-pool	221
	lu	223
	mapping	225
	port	227
Delete	Suprime los elementos siguientes:	228
	<ul style="list-style-type: none"> • implicit-pool • lu • mapping • port 	
List all	Lista la memoria de configuración	230
Exit	Le devuelve al nivel de mandatos anterior. Consulte la sección "Cómo salir de un entorno de nivel inferior" en la página xxix.	

Sintaxis:

set

Se le solicitará que entre los valores de los parámetros siguientes. El rango del parámetro se mostrará entre paréntesis (). El valor por omisión del parámetro se mostrará entre corchetes [].

Tabla 41 (Página 1 de 4). Lista de parámetros de configuración - Establecimiento de TN3270E

Información de los parámetros	
Parámetro	Enable TN3270E Server
Valores válidos	Yes o No
Valor por omisión	Yes
Descripción	Este parámetro especifica si se habilitará el soporte al servidor de TN3270E.

<i>Tabla 41 (Página 2 de 4). Lista de parámetros de configuración - Establecimiento de TN3270E</i>	
Información de los parámetros	
Parámetro	TN3270E Server IP Address
Valores válidos	Se acepta cualquier dirección IP como entrada válida. Sin embargo, la dirección también debe estar configurada en IP como dirección de interfaz o como dirección IP interna del direccionador.
Valor por omisión	Ninguno
Descripción	Este parámetro es la dirección IP asociada al servidor de TN3270E.
Parámetro	Port number
Valores válidos	De 1 a 65535
Valor por omisión	23
Descripción	Este parámetro especifica el número de puerto asociado al servidor de TN3270E.
Parámetro	Enable Client IP address to LU name mapping?
Valores válidos	Yes o No
Valor por omisión	No
Descripción	Este parámetro especifica si se produce la correlación de dirección IP de cliente con nombre de LU.
Parámetro	Default pool name
Valores válidos	Cualquier serie alfanumérica de 1 a 8 caracteres
Valor por omisión	PUBLIC
Descripción	Este parámetro especifica el nombre de la agrupación por omisión. Esta agrupación se usa cuando los clientes de TN3270 se conectan y no especifican un nombre de agrupación/LU.
Parámetro	NetDisp Advisor Port Number
Valores válidos	De 1 a 65535
Valor por omisión	10008
Descripción	Este parámetro establece el número de puerto de Network Dispatcher Advisor.

Mandatos de configuración de APPN

Tabla 41 (Página 3 de 4). Lista de parámetros de configuración - Establecimiento de TN3270E	
Información de los parámetros	
Parámetro	Keepalive type
Valores válidos	<p>0 Ninguno</p> <p>1 Timing mark (Marca de temporización)</p> <p>2 NOP</p>
Valor por omisión	0
Descripción	<p>Este parámetro especifica el tipo de Keepalive.</p> <p>El tipo de Keepalive que corresponde a <i>Timing mark</i> requiere respuestas del cliente dentro del plazo de tiempo especificado con el parámetro Timer (Temporizador).</p> <p>El tipo de Keepalive <i>NOP</i> especifica que el cliente no devolverá una respuesta al mensaje Keepalive. La notificación de que el cliente ya no está allí proviene de TCP.</p>
Parámetro	Frequency
Valores válidos	De 1 a 65535 segundos
Valor por omisión	60
Descripción	Este parámetro especifica la frecuencia con que se envía un mensaje Keepalive al cliente.
Parámetro	Timer
Valores válidos	De 1 a 65535 segundos
Valor por omisión	10
Descripción	Este parámetro establece el valor del temporizador que se usará con la función Keepalive.
Parámetro	Automatic logoff
Valores válidos	Yes o No
Valor por omisión	No
Descripción	Este parámetro especifica si se habilitará la desconexión automática.
Parámetro	Time
Valores válidos	De 1 a 65535 minutos
Valor por omisión	30
Descripción	Este parámetro establece el tiempo en que puede estar desocupado el enlace TN3270E antes de que se desconecte automáticamente.
Parámetro	IPv4 Precedence
Valores válidos	Yes o No
Valor por omisión	No
Descripción	Este parámetro establece el valor de precedencia de IPv4, lo que permite la puesta en cola prioritaria de paquetes encapsulados IPv4.

Tabla 41 (Página 4 de 4). Lista de parámetros de configuración - Establecimiento de TN3270E

Información de los parámetros	
Parámetro	Enable LU Capping?
Valores válidos	Yes o No
Valor por omisión	No
Descripción	Este parámetro permite determinar el número de sesiones TN3270 que cada dirección IP tiene permiso para iniciar. Si la respuesta a esta pregunta es yes, aparecerá la pregunta siguiente.
Parámetro	Max number of LUs per IP address
Valores válidos	De 0 a 65535
Valor por omisión	0
Descripción	Este parámetro establece el número máximo de sesiones TN3270 que cada dirección IP de cliente tiene permiso para iniciar.

Sintaxis:

add implicit-pool

Este mandato define una agrupación de LU en oposición al mandato **add lu** que añade una LU única. Se le solicitará que entre los valores de los parámetros siguientes. El rango del parámetro se mostrará entre paréntesis (). El valor por omisión del parámetro se mostrará entre corchetes [].

Tabla 42 (Página 1 de 3). Lista de parámetros de configuración - Añadir TN3270E implícito

Información de los parámetros	
Parámetro	Pool name
Valores válidos	Una serie de 1 a 8 caracteres: <ul style="list-style-type: none"> • Primer carácter: De la A a la Z, \$, #, @, ó < • Del segundo al octavo carácter: De la A a la Z, de 0 a 9, \$, #, @, > ó <
Valor por omisión	PUBLIC
Descripción	Este parámetro especifica el nombre de la agrupación de LU que se usará cuando los clientes de TN3270 se conecten.
Parámetro	Pool class
Valores válidos	1 ó 2, donde: <ol style="list-style-type: none"> 1. Estación de trabajo implícita 2. Impresora implícita
Valor por omisión	1
Descripción	Este parámetro especifica el tipo de agrupación de LU.

Mandatos de configuración de APPN

<i>Tabla 42 (Página 2 de 3). Lista de parámetros de configuración - Añadir TN3270E implícito</i>	
Información de los parámetros	
Parámetro	Station name
Valores válidos	Una serie de 1 a 8 caracteres: <ul style="list-style-type: none"> • Primer carácter: De la A a la Z • Del segundo al octavo carácter: De la A a la Z, de 0 a 9
Valor por omisión	Ninguno
Descripción	Este parámetro especifica el nombre que representa el enlace entre el DLUR y la PU o el enlace de subárea sobre el que fluirán los datos de SNA.
Parámetro	LU Name Mask
Valores válidos	Una serie de 1 a 5 caracteres: <ul style="list-style-type: none"> • Primer carácter: De la A a la Z, @, \$ y # • Del segundo al octavo carácter: De la A a la Z, de 0 a 9
Valor por omisión	@01LU
Descripción	Este parámetro especifica la máscara que se usará para asegurarse de que los nombres de LU no dupliquen otros nombres de la red. Los nombres de LU se generan añadiendo la dirección NAU al final de la máscara de nombre de la LU. Cuando no se especifica un rango de dirección, se comprobarán las direcciones de NAU de 2 a 253 para ver si la dirección está sin usar. Si la dirección está disponible, se usará. De lo contrario, se intentará la siguiente dirección NAU. Por ejemplo, si la máscara de LU es FRED, los nombres de LU posible son [FRED2, FRED3, ..., FRED253].
Parámetro	LU type
Valores válidos	<ul style="list-style-type: none"> • 1 - Pantalla 3270 mod 2 • 2 - Pantalla 3270 mod 3 • 3 - Pantalla 3270 mod 4 • 4 - Pantalla 3270 mod 5 • 5 - Impresora 3270 • 6 - Impresora SCS
Valor por omisión	1
Descripción	Este parámetro especifica el tipo de LU dependiente para la LU que se está añadiendo.
Parámetro	Specify LU address range?
Valores válidos	Yes o No
Valor por omisión	No
Descripción	Este parámetro especifica si desea definir un rango de dirección de LU.

Tabla 42 (Página 3 de 3). Lista de parámetros de configuración - Añadir TN3270E implícito

Información de los parámetros	
Parámetro	LU address range
Valores válidos	Cualquier rango de valores comprendidos entre 1 y 255
Valor por omisión	ninguno
Descripción	<p>Este parámetro especifica el rango de dirección de LU.</p> <p>La dirección de LU puede especificarse usando el formato siguiente:</p> <p style="text-align: center;">frontera_dirección_inferior-frontera_dirección_superior</p> <p>Si no hay ningún guión después del primer valor, se supone que el valor es una dirección de LU única. Pueden entrarse varios rango separados por comas. Por ejemplo, la serie siguiente especifica 2 rangos de direcciones y 2 direcciones de LU específicas:</p> <p style="text-align: center;">2-40,56,58,100-250</p>
Parámetro	Number of implicit workstation definitions
Valores válidos	De 1 a 255
Valor por omisión	1
Descripción	Este parámetro especifica el número de LU dependientes que se añadirán a la agrupación implícita.

add

lu

Este mandato añade una LU específica. Se le solicitará que entre los valores de los parámetros siguientes. El rango del parámetro se mostrará entre paréntesis (). El valor por omisión del parámetro se mostrará entre corchetes [].

Tabla 43 (Página 1 de 3). Lista de parámetros de configuración - Añadir LU TN3270E

Información de los parámetros	
Parámetro	LU name
Valores válidos	<p>Una serie de 1 a 8 caracteres:</p> <ul style="list-style-type: none"> • Primer carácter: De la A a la Z, @, \$ y # • Del segundo al octavo carácter: De la A a la Z, de 0 a 9
Valor por omisión	Ninguno
Descripción	Este parámetro especifica el nombre de LU de la LU dependiente que se está definiendo.
Parámetro	NAU address
Valores válidos	De 1 a 255
Valor por omisión	Ninguno
Descripción	Este parámetro especifica la dirección NAU de la LU que se está definiendo.

Mandatos de configuración de APPN

Tabla 43 (Página 2 de 3). Lista de parámetros de configuración - Añadir LU TN3270E	
Información de los parámetros	
Parámetro	Station name
Valores válidos	Una serie de 1 a 8 caracteres: <ul style="list-style-type: none"> • Primer carácter: De la A a la Z • Del segundo al octavo carácter: De la A a la Z, de 0 a 9
Valor por omisión	Ninguno
Descripción	Este parámetro especifica el nombre que representa el enlace entre el DLUR y la PU definido usando el mandato add local-pu o el enlace de subárea sobre el que fluirán los datos de SNA.
Parámetro	Class
Valores válidos	<ul style="list-style-type: none"> 1 Estación de trabajo explícita 2 Estación de trabajo implícita 3 Impresora explícita 4 Impresora implícita
Valor por omisión	1
Descripción	Este parámetro especifica la clase de LU.
Parámetro	LU type
Valores válidos	<ul style="list-style-type: none"> • 1 — Pantalla 3270 mod 2 • 2— Pantalla 3270 mod 3 • 3 — Pantalla 3270 mod 4 • 4 — Pantalla 3270 mod 5 • 5 — Impresora 3270 • 6 — Impresora SCS
Valor por omisión	1
Descripción	Este parámetro especifica el tipo de LU dependiente para la LU que se está añadiendo.
Parámetro	Implicit pool name
Valores válidos	Una serie de 1 a 8 caracteres: <ul style="list-style-type: none"> • Primer carácter: De la A a la Z, < • Del segundo al octavo carácter: De la A a la Z, de 0 a 9
Valor por omisión	<DEFLT>
Descripción	Este parámetro especifica el nombre de la agrupación implícita que se usará en la definición de la LU. Sólo se hace esta pregunta si <i>class</i> es una estación de trabajo o una impresora implícita.
Parámetro	Define an associated printer
Valores válidos	Yes o No
Valor por omisión	No
Descripción	Este parámetro especifica si desea definir una impresora asociada.

Tabla 43 (Página 3 de 3). Lista de parámetros de configuración - Añadir LU TN3270E	
Información de los parámetros	
Parámetro	Associated printer name
Valores válidos	Una serie de 1 a 8 caracteres: <ul style="list-style-type: none"> • Primer carácter: De la A a la Z, @, \$ y # • Del segundo al octavo carácter: De la A a la Z, de 0 a 9
Valor por omisión	Ninguno
Descripción	Este parámetro especifica el nombre de la impresora asociada.
Parámetro	Associated printer NAU address
Valores válidos	De 1 a 255
Valor por omisión	Ninguno
Descripción	Este parámetro especifica la dirección NAU para la definición de LU de la impresora asociada.

Sintaxis:

add map

Este mandato añade una correlación de dirección IP de cliente con nombre de LU. Se le solicitará que entre los valores de los parámetros siguientes. El rango del parámetro se mostrará entre paréntesis (). El valor por omisión del parámetro se mostrará entre corchetes [].

Se aplican las normas de correlación siguientes:

- Si una definición de correlación contiene una máscara de subred completa (255.255.255.255) que indica que la entrada es para un cliente específico y el cliente no solicita una LU/grupación específica, podrá intentarse cualquier LU/grupación de la definición de correlación que coincida con el tipo de conexión.
- Si una definición de correlación no contiene una máscara de subred completa y no se solicita una LU/grupación específica, sólo se intentarán las entradas de la agrupación de la definición de correlación. No puede crear una definición que correlacione una subred con una LU específica. Debe correlacionar la subred con una agrupación.
- Si se recibe una solicitud de conexión de un cliente y no hay entradas de correlación que coincidan, se rechazará la solicitud.
- Puede añadirse una mezcla de tipos de LU y agrupaciones a una correlación determinada. El recurso seleccionado se basará en el tipo de solicitud de conexión. El orden seguido en la definición de los recursos en la correlación será el seguido para elegir el recurso para una solicitud de conexión determinada.
- Si una definición de correlación contiene un número de puerto de destino que no es cero, sólo se comprobarán los clientes que se conectan a ese puerto respecto a dicha correlación.

Nota: Cuando un cliente se conecta mientras está habilitada la correlación, el servidor empezará a ejecutar AND de la dirección IP del cliente con la máscara de subred de cada correlación secuencial. La coincidencia más larga entre la dirección IP del cliente de entrada y la definición de correlación determinará qué definición de correlación se intentará primero. Si se están utilizando todos los recursos elegibles de la definición de correlación y **final LU mapping connection attempt** es *no*, se buscará de nuevo en las definiciones de correlaciones para encontrar la siguiente coincidencia más específica.

Tabla 44 (Página 1 de 2). Lista de parámetros de configuración - Añadir correlación de TN3270E	
Información de los parámetros	
Parámetro	Pool name/LU name
Valores válidos	Una serie de 1 a 8 caracteres: <ul style="list-style-type: none"> • Primer carácter: De la A a la Z • Del segundo al octavo carácter: De la A a la Z, de 0 a 9
Valor por omisión	Ninguno
Descripción	Este parámetro especifica un nombre de LU o un nombre de agrupación que se correlacionará con la dirección IP. El nombre de LU sólo puede correlacionarse con una dirección de sistema principal. Si la máscara es una máscara de red, el nombre especificado deberá ser un nombre de agrupación.
Parámetro	Client IP address or Network address
Valores válidos	Cualquier dirección IP válida
Valor por omisión	0.0.0.0
Descripción	Este parámetro especifica la definición de dirección IP del cliente o de correlación de red que debe añadirse.
Parámetro	Address Mask
Valores válidos	Cualquier máscara de dirección IP válida
Valor por omisión	0.0.0.0
Descripción	Este parámetro especifica la máscara de dirección IP que el direccionador aplica a las direcciones IP entrantes de cliente y direcciones de red o cliente IP configuradas para determinar si coinciden.
Parámetro	Port number
Valores válidos	De 1 a 65535 Si desea especificar un puerto específico, deberá seleccionar el valor del puerto de servidor de TN3270 global definido con el mandato set o uno de los valores de puerto definidos con el mandato add port .
Valor por omisión	0
Descripción	Este parámetro especifica el número de puerto TCP de destino al que un cliente de TN3270 debe conectarse para que se compruebe esta entrada de correlación. Si el valor es cero, la entrada de correlación es aplicable a las conexiones de cliente con cualquier número de puerto TCP definido.

Tabla 44 (Página 2 de 2). Lista de parámetros de configuración - Añadir correlación de TN3270E

Información de los parámetros	
Parámetro	Final LU mapping connection attempt
Valores válidos	Yes o No
Valor por omisión	No
Descripción	Este parámetro especifica si el direccionador debe continuar probando entradas de correlación menos específicas si una coincidencia de cliente con esta entrada no ha conseguido dar una LU disponible válida.

Sintaxis:

add port

Este mandato especifica el puerto adicional que el servidor de TN3270E escuchará. Se le solicitará que entre los valores de los parámetros siguientes. El rango del parámetro se mostrará entre paréntesis (). El valor por omisión del parámetro se mostrará entre corchetes [].

Tabla 45 (Página 1 de 2). Lista de parámetros de configuración - Añadir puerto de TN3270E

Información de los parámetros	
Parámetro	Port number
Valores válidos	De 1 a 65535
Valor por omisión	ninguno
Descripción	Este parámetro especifica el número de puerto que debe añadirse.
Parámetro	Support TN3270E?
Valores válidos	Yes o No
Valor por omisión	Yes
Descripción	Este parámetro especifica si el puerto añadido negociará para ser un servidor de TN3270E. Si no es un servidor de "E", no dará soporte a las solicitudes de impresión o del sistema.
Parámetro	Pool name
Valores válidos	Una serie de 1 a 8 caracteres: <ul style="list-style-type: none"> • Primer carácter: De la A a la Z • Del segundo al octavo carácter: De la A a la Z, de 0 a 9
Valor por omisión	Ninguno
Descripción	Este parámetro especifica el nombre de la agrupación asociada a este puerto. A los clientes que se conecten con este puerto y no especifiquen ningún nombre de LU o de agrupación, se les asignará una LU de esta agrupación.

Mandatos de configuración de APPN

Tabla 45 (Página 2 de 2). Lista de parámetros de configuración - Añadir puerto de TN3270E

Información de los parámetros	
Parámetro	Disable Client Filtering for this port?
Valores válidos	Yes o No
Valor por omisión	No
Descripción	Este parámetro especifica si las conexiones de entrada de este puerto deben usar la función de correlación de la dirección IP del cliente de caja con el nombre de la LU, si está habilitada.

Sintaxis:

delete lu

Este mandato elimina LU TN3270E. Se le solicitará que entre los valores de los parámetros siguientes. El rango del parámetro se mostrará entre paréntesis (). El valor por omisión del parámetro se mostrará entre corchetes [].

Tabla 46. Lista de parámetros de configuración - Suprimir LU de TN3270E

Información de los parámetros	
Parámetro	LU name
Valores válidos	Una serie de 1 a 8 caracteres: <ul style="list-style-type: none">• Primer carácter: De la A a la Z, @, \$ y #• Del segundo al octavo carácter: De la A a la Z, de 0 a 9
Valor por omisión	Ninguno
Descripción	Este parámetro especifica el nombre de LU de la LU dependiente que se va a eliminar.

Sintaxis:

delete implicit-pool

Este mandato elimina una agrupación implícita de TN3270E. Se le solicitará que entre los valores de los parámetros siguientes. El rango del parámetro se mostrará entre paréntesis (). El valor por omisión del parámetro se mostrará entre corchetes [].

Tabla 47 (Página 1 de 2). Lista de parámetros de configuración - Supresión de TN3270E implícita

Información de los parámetros	
Parámetro	Pool name
Valores válidos	Una serie de 1 a 8 caracteres: <ul style="list-style-type: none">• Primer carácter: De la A a la Z• Del segundo al octavo carácter: De la A a la Z, de 0 a 9
Valor por omisión	Ninguno
Descripción	Este parámetro especifica el nombre de la agrupación de LU que se va a suprimir.

<i>Tabla 47 (Página 2 de 2). Lista de parámetros de configuración - Supresión de TN3270E implícita</i>	
Información de los parámetros	
Parámetro	Delete entire pool
Valores válidos	Yes o No
Valor por omisión	No
Descripción	Este parámetro especifica si se va a suprimir toda la agrupación o una entrada específica.
Parámetro	Station name
Valores válidos	Una serie de 1 a 8 caracteres: <ul style="list-style-type: none"> • Primer carácter: De la A a la Z • Del segundo al octavo carácter: De la A a la Z, de 0 a 9
Valor por omisión	Ninguno
Descripción	Este parámetro especifica el nombre de la estación que se va a suprimir.

Sintaxis:

delete map

Este mandato elimina una correlación de dirección IP de cliente con nombre de LU. Se le solicitará que entre los valores de los parámetros siguientes. El rango del parámetro se mostrará entre paréntesis (). El valor por omisión del parámetro se mostrará entre corchetes [].

<i>Tabla 48 (Página 1 de 2). Lista de parámetros de configuración - Suprimir correlación de TN3270E</i>	
Información de los parámetros	
Parámetro	Client IP address or Network address
Valores válidos	Cualquier dirección IP válida
Valor por omisión	0.0.0.0
Descripción	Este parámetro especifica la definición de dirección IP del cliente o de correlación de red que debe suprimirse.
Parámetro	Client IP address or Network address Mask
Valores válidos	Cualquier máscara de dirección IP válida
Valor por omisión	0.0.0.0
Descripción	Este parámetro especifica la definición de máscara de dirección IP del cliente o de correlación de red que debe suprimirse.
Parámetro	Delete all entries for this client?
Valores válidos	Yes o No
Valor por omisión	No
Descripción	Este parámetro especifica si se va a suprimir toda la agrupación o un nombre específico.

Tabla 48 (Página 2 de 2). Lista de parámetros de configuración - Suprimir correlación de TN3270E

Información de los parámetros	
Parámetro	Pool name
Valores válidos	Una serie de 1 a 8 caracteres: <ul style="list-style-type: none"> • Primer carácter: De la A a la Z • Del segundo al octavo carácter: De la A a la Z, de 0 a 9
Valor por omisión	Ninguno
Descripción	Este parámetro especifica el nombre de LU o el nombre de agrupación que se va a eliminar.

Sintaxis:

delete port

Este mandato suprime definiciones de puerto. Se le solicitará que entre los valores de los parámetros siguientes. El rango del parámetro se mostrará entre paréntesis (). El valor por omisión del parámetro se mostrará entre corchetes [].

Tabla 49. Lista de parámetros de configuración - Suprimir puerto de TN3270E

Información de los parámetros	
Parámetro	Port number
Valores válidos	De 1 a 65536
Valor por omisión	ninguno
Descripción	Este parámetro especifica el número de puerto que debe añadirse.

Sintaxis:

list all

Este mandato lista una configuración de TN3270E.

Supervisión de APPN

Esta sección describe cómo supervisar APPN. Está formada por las secciones siguientes:

- “Acceso a los mandatos de supervisión de APPN”
- “Mandatos de supervisión de APPN” en la página 231

Acceso a los mandatos de supervisión de APPN

Siga el procedimiento siguiente para acceder a los mandatos de supervisión de APPN. Este proceso le dará acceso a un proceso de *supervisión* de APPN.

En el indicador OPCON, entre **talk 5**.

Después de entrar el mandato **talk 5**, el indicador de GWCON (+) aparecerá en el terminal. Si el indicador no aparece cuando entre por primera vez la configuración, pulse de nuevo **Retorno**.

Entre **protocolo APPN**. Por ejemplo:

```
* talk 5
+
+ protocol APPN
APPN>
```

Si al escribir **p appn** se obtiene el mensaje “Protocol APPN is available but not configured” (El protocolo APPN está disponible pero no está configurado), probablemente tiene uno de los errores siguientes:

- No ha habilitado APPN globalmente en la configuración activa (aunque puede que haya configurado parámetros APPN). Compruebe la configuración actual y, si éste es el caso, habilite APPN y vuelva a iniciar o cargar el direccionador.
- La cantidad de memoria necesaria para que APPN se inicialice debidamente no estaba disponible en el direccionador. Utilice **talk 2** para ver si se ha registrado un mensaje de error correspondiente a este defecto. Si es así, vuelva a configurar APPN de modo que utilice menos memoria y vuelva a iniciar o cargar el direccionador.

Cuando haya llegado al indicador de supervisión de APPN, entre **tn3270** para llegar al indicador de supervisión TN3270E >.

Mandatos de supervisión de APPN

Esta sección describe los mandatos de supervisión de APPN para supervisar las interfaces de APPN. Entre los mandatos en el indicador APPN> y los mandatos del servidor de TN3270 en el indicador TN3270E>.

Tabla 50 (Página 1 de 3). Resumen de los mandatos de supervisión de APPN

Mandato	Función	Consulte más detalles en la página:
? (Help)	Muestra todos los mandatos disponibles para este nivel de mandatos o lista las opciones de palabras clave para mandatos específicos.	--
activate link	Activa un enlace configurado.	“Activate” en la página 235
aping	Prueba la conectividad SNA/APPN con una LU de destino.	“Aping” en la página 235
deactivate link	Desactiva un enlace configurado o dinámico.	“Deactivate link” en la página 236
list cp-cp_sessions	Muestra una lista de todos los CP adyacentes que puedan tener sesiones de CP-CP con este direccionador.	página 239
list dlur dlus	Muestra una lista de DLUS activos y el estado de cada sesión en el conducto DLUS-DLUR.	página 239
list dlur lu	Muestra una lista de PU internas o en sentido directo con estadísticas de LU para cada PU.	página 240
list dlur pu	Muestra una lista de PU internas o en sentido directo con su estado de conexión.	página 241

Mandatos de supervisión de APPN

<i>Tabla 50 (Página 2 de 3). Resumen de los mandatos de supervisión de APPN</i>		
list dlur status	Muestra un resumen de información de configuración del DLUR global actualmente activo.	página 242
list ds incomplete_locates	Muestra una lista de búsquedas APPN que están actualmente en curso.	página 243
list ds resource	Muestra una lista completa o parcial de nombres de LU del directorio APPN de este direccionador.	página 243
list ds status	Muestra un resumen de estadísticas del directorio de servicios APPN.	página 245
list focal	Muestra una lista de puntos focales de gestión de la red y también el estado de los mismos.	página 245
list isr_sessions	Muestra el número de sesiones ISR LU-LU activas que pasan a través de este direccionador, por enlace.	página 246
list link	Muestra una lista de enlaces configurados y dinámicos desde este direccionador.	página 247
list link <i>nombre-enlace</i>	Muestra la configuración y el estado detallados de un enlace específico.	página 248
list local_link	Muestra una lista de enlaces lógicos desde el DLUR a las PU2.0 de este direccionador (que se utilizan para contener las LU de TN3270).	página 250
list log	Ahora se ha substituido por "log view" y "log status".	página 262
list port	Muestra una lista de puertos de direccionador APPN lógicos y físicos configurados, y también su estado.	página 250
list port <i>nombre-puerto</i>	Muestra la configuración y el estado detallados de un puerto específico.	página 251
list rtp	Muestra una lista de nodos en la tabla de asociados RTP y un resumen de información acerca de todas las conexiones RTP activas.	página 252
list rtp <i>tcid</i>	Muestra información detallada acerca de una o todas las conexiones RTP.	página 255
list session	Muestra una lista de sesiones ISR que fluyen a través del direccionador.	página 256

Mandato	Función	Consulte más detalles en la página:
list status	Muestra un resumen de configuración APPN general y de información de estado.	página 257
list topo node	Muestra información de la base de datos de topología de este direccionador sobre un nodo específico de esta subred de topología.	página 258
list topo status	Muestra un resumen de estadísticas de base de datos de topología.	página 260
list topo tg	Muestra una lista completa o parcial de TG activos de esta subred de topología.	página 260
log status	Muestra un resumen de información sobre el registro cronológico de sucesos APPN.	página 262
log view	Entra un submenú para navegar y ver entradas de registro cronológico de sucesos APPN.	página 262
memory	Muestra un resumen de información e información detallada sobre el uso de memoria APPN dentro del direccionador.	"Memory" en la página 266
restart	Detiene y reactiva APPN y TN3270 con una interrupción.	"Restart" en la página 271
rtp status	Muestra información de la configuración RTP global que se encuentra en uso actualmente.	"Rtp status" en la página 269
rtp switchpath	Ocasiona una conmutación de conexión RTP al mejor recorrido actualmente disponible.	"Rtp switchpath" en la página 269
rtp test	Efectúa una prueba de direccionamiento HPR y muestra los resultados.	"Rtp test" en la página 270
stop	Detiene APPN y TN3270 con una interrupción.	"Stop" en la página 271
test rtp	Efectúa una prueba de direccionamiento HPR y muestra los resultados (forma antigua correspondiente a "rtp test").	"Rtp test" en la página 270
tn3270e	Accede al menú de mandato de supervisión de TN3270.	"Mandatos de supervisión de TN3270E" en la página 271
exit	Le devuelve al menú de supervisión principal de Talk 5.	--

Mandato	Función	Consulte más detalles en la página:
---------	---------	-------------------------------------

Mandatos de supervisión de APPN

<i>Tabla 51 (Página 2 de 2). Resumen de los mandatos de supervisión del servidor de TN3270E</i>		
? (Help)	Muestra todos los mandatos disponibles para este nivel de mandatos o lista las opciones de palabras clave para mandatos específicos.	--
deactivate lu	Desactiva por la fuerza una LU en uso por parte de un cliente de TN3270 y desconecta la conexión TCP correspondiente con dicho cliente.	"Deactivate LU" en la página 272
list connections	Muestra una lista completa o parcial de conexiones de cliente activas.	273
list lu <i>nombre-lu</i>	Muestra información detallada de configuración y estado de una única LU interna.	274
list mapping	Muestra una lista de correlaciones de direcciones IP de cliente con nombres de agrupación/LU configuradas.	275
list pools	Muestra una lista de agrupaciones de LU implícitas configuradas.	276
list pools <i>nombre-agrupación</i>	Muestra información detallada acerca de una única agrupación de LU.	276
list ports	Muestra una lista de puertos TCP de destino configurados del servidor de TN3270.	278
list pu	Muestra una lista de todas las PU internas (tanto de DLUR como de subárea) con un resumen la información de estado y configuración.	278
list pu <i>nombre-pu</i>	Muestra una lista de todas las LU internas bajo la PU especificada, con un resumen de la información de estado y de configuración para cada LU.	279
list rejections	Muestra una lista de las conexiones de cliente más recientes que han sido rechazadas.	280
list status	Muestra un resumen estadístico y la configuración del servidor de TN3270 global.	281
exit	Le devuelve al menú de supervisión de APPN.	--

Detalles de los mandatos de supervisión de APPN

Esta sección describe la sintaxis detallada de los mandatos de supervisión de APPN. Entre estos mandatos en el indicador de mandatos APPN>.

Activate

Use el mandato **activate link** para activar un enlace configurado. Use el mandato **list link** para buscar el nombre del enlace que desee activar y para ver el estado del enlace después de activarlo.

Sintaxis:

activate link *nombre_enlace*

Aping

Use el mandato **aping** para enviar un mensaje a otra dirección y esperar una respuesta.

Nota: Cuando APING responda en menos de 1 milisegundo, la velocidad de los datos mostrada aparecerá como "-----".

Sintaxis:

aping *pares distintivo-valor nombre_lu*

donde,

pares distintivo-valor

Especifica uno o más de los siguientes distintivos seguidos de un valor. Especifique estos valores de distintivo sólo si desea alterar temporalmente los valores por omisión.

Distintivo	Significado	Valor por omisión
-m	Nombre de modalidad para una sesión LU6.2	#INTER
-t	Nombre del TP (programa de transacción) de destino	APING
-i	Cuenta de envíos y recepciones a emitir	1
-x	Cuenta de conversaciones LU6.2 a ejecutar (en serie)	1
-y	Cuenta de los TP a ejecutar (en serie)	1
-s	Tamaño del paquete	100 bytes
-q	Lacónico	Mensajes de estado
-b	La visualización de salida va a talk 2 (en el fondo)	Visualizar a Talk 5

Mandatos de supervisión de APPN

nombre_lu

Especifica el nombre de LU plenamente calificado del destino de APING.

Valores válidos: Cualquier nombre de LU plenamente calificado válido

Ejemplo:

```
APPN >aping stfnet.mvs8
Allocate duration: 536 msec
Iteration Duration Data Sent Data Rate
number (msec) (bytes) (Kb/s) LU name
-----
0 458 100 1 STFNET.MVS8
-----
Avg. 458 100 1
```

Tabla 53. Descripción de la salida de APING

Elemento	Descripción	Valores clave
Allocate duration	Tiempo necesario para configurar la sesión de LU6.2 y la conversación para el aping.	--
Iteration duration	Tiempo total necesario para enviar y recibir un acuse de recibo para el paquete de datos.	--
Iteration data rate	Velocidad de datos calculada (mín. 1Kb/s) en base a la duración y a los bytes enviados.	--

Deactivate link

Use el mandato **deactivate link** para desactivar un enlace configurado. Use el mandato **list link** para ver nombres de enlace y para ver el estado del enlace después de utilizar este mandato. Los enlaces configurados deben estar inactivos y los enlaces dinámicos deben desaparecer.

Sintaxis:

deactivate link nombre_enlace

Dump

Use el mandato **Dump** para crear un vuelco APPN. Puede usar **Boot config** en **talk 6** para determinar dónde se guardará el vuelco. El nombre del vuelco será el mismo que el vuelco del direccionador completo con '_A.1' concatenado al final. Puede iniciar varios vuelcos. La concatenación se incrementará por cada vuelco. Cuando el nombre del vuelco haya llegado a '_A.5', se restablecerá en '_A.1'.

Sintaxis:

dump

Debido a que este vuelco no interrumpe las funciones APPN, se puede mejorar su integridad minimizando mandatos de control APPN y tráfico mientras el vuelco está en curso.

List

Use el mandato **List** para visualizar información sobre la configuración de APPN.
El mandato lista:

Sintaxis:**list**

appc_sessions
 cp-cp_sessions
 dlur dlus
 dlur lu
 dlur pu
 dlur status
 ds incomplete_locates
 ds resource
 ds status
 dumps
 focal
 isr_sessions
 link
 link *nombre-enlace*
 local_link
 log
 port
 port *nombre-puerto*
 rtp
 rtp *tcid*
 session
 status
 topo node
 topo status
 topo tg

Mandato Función**list appc_sessions**

Use el mandato **list appc** para visualizar una lista de todas las sesiones LU6.2 que tienen un punto final en este direccionador. Algunos ejemplos de estas sesiones son:

Mandatos de supervisión de APPN

sesiones de CP-CP, sesiones de DLUR a DLUS, sesiones hacia un punto focal de gestión de red y sesiones iniciadas debido a un mandato "aping". Este mandato lista todas las sesiones activas. Si un conducto consta de dos sesiones unidireccionales, se visualizan ambas sesiones del par.

Ejemplo:

```
APPN >li appc
LU Name           Mode Type FSM FID PCID
=====
STFNET.CP3174BC   CPSVCMG Pri  ACT  FID2 C4 9B 1F 3B 03 54 83 3D
STFNET.CP3174BC   CPSVCMG Sec  ACT  FID2 CB 13 AF 4A 23 AC E5 06
STFNET.VL14       CPSVCMG Pri  ACT  FID5 C4 9B 1F 3B 03 54 83 40
STFNET.VL14       CPSVCMG Sec  ACT  FID5 CB 67 9F CA F8 27 B5 9F
STFNET.VLNN045    CPSVCMG Sec  ACT  FID5 C8 8B 1F 3B 04 42 34 FA
STFNET.VLNN045    CPSVCMG Pri  ACT  FID5 C4 9B 1F 3B 03 54 83 41
STFNET.MVS8       CPSVRMGR Pri  ACT  FID2 C4 9B 1F 3B 03 54 83 42
STFNET.MVS8       CPSVRMGR Sec  ACT  FID2 D3 B7 7C D5 57 35 0B C8
```

Tabla 54. Descripción de la salida de list appc_sessions

Elemento	Descripción	Valores clave
LU name	Nombre de LU de un asociado completamente calificado	--
Mode	Nombre de modalidad de la sesión	<ul style="list-style-type: none"> • #CONNECT = prioridad media normal • #INTER = prioridad media alta • CPSVCMG = sesión de CP-CP • CPSVRMGR = sesión de DLUR-DLUS • SNASVCMG = sesión de punto focal • otros nombres de modalidad tienen una arquitectura y también pueden ser definidos por el usuario
Type	Función de activación de la sesión de direccionador	<ul style="list-style-type: none"> • Pri = Primario • Sec = Secundario
FSM	Estado de la sesión actual (valor Finite State Machine)	<ul style="list-style-type: none"> • ACT = activo • PBIR = solicitud BIND pendiente • PCIN = CINIT pendiente (Servicios de sesiones está buscando y encontrando el TG de salida) • RES = reset (inicial)
FID	Tipo de ID de formato	<ul style="list-style-type: none"> • FID2 = ISR • FID5 = HPR
PCID	ID de correlacionador de procedimientos: identificador de sesión	--

list cp-cp_sessions

Use el mandato **list cp** para visualizar una lista de todos los nodos adyacentes que pueden tener sesiones de CP-CP con este direccionador. La lista de salida incluye todos los CP que tienen un enlace activo que soporta sesiones de CP-CP, así como también CP que ya no están conectados pero que han tenido un enlace capacitado para CP-CP (desde que APPN se ha reiniciado por última vez). A diferencia del mandato **list appc**, una línea de datos de salida representa un par de sesión conwinner/conloser.

Si el direccionador está configurado como nodo de Branch Extender, la lista indicará sólo un par de sesión de CP-CP activo a un NN adyacente. Es el servidor NN del nodo BEX.

Ejemplo:

```
APPN >li cp
      CP Name Type      Status      ConWinner ConLoser ConWinner ConLoser
      ID      Sense      Sense
-----
      STFNET.NN12  NN      Active    BAF92A69  BAF92A84  080F6051  00000000
      STFNET.CP3174BC  NN      Active    BAF927E3  BAF927E5  00000000  00000000
```

Tabla 55. Descripción de la salida

Elemento	Descripción	Valores clave
CP name	Nombre plenamente calificado de un CP adyacente	--
Type	Tipo de nodo de un CP adyacente	NN = nodo de red EN = nodo final Virt = nodo virtual
Status	Estado del par de sesión de CP-CP	Active Inactive Pending
ConWinner/Loser ID	ID de sesión interna del direccionador para la sesión ganador/perdedor de la contienda en el par de sesión de CP-CP, 0 si la sesión no está conectada	--
ConWinner/Loser sense	Código de detección SNA indicando el motivo por el que la sesión de conwinner/loser se desconectó por última vez.	--

list dlur dlus

Use el mandato **list dlur dlus** para visualizar una lista de DLUS activos y el estado de cada sesión en el conducto DLUR-DLUS. Los DLUS listados pueden venir de uno de estos orígenes:

- Configurado en el direccionador como DLUS de seguridad o primario global
- Configurado en el direccionador como DLUS primario o de seguridad para un enlace en sentido directo específico

Mandatos de supervisión de APPN

- DLUS dinámico (no configurado) que conecta con el direccionador y conduce la llamada a las PU dependientes.

Ejemplo:

```
APPN >1i dlur dlus
DLUS  NAME                CONWINNER  CONLOSER
      STATE                STATE
-----
STFNET.MVS8              UP          UP
```

Tabla 56. Descripción de la salida de list dlur-dlus

Elemento	Descripción	Valores clave
DLUS name	Nombre de CP plenamente calificado del DLUS	--
ConWinner/Loser state	Estado de la contienda de sesión ganador/perdedor en el par de sesión de DLUR-DLUS	UP DOWN PENDING_UP PENDING_DOWN BLOCKED = esperando la entrada en función de SSCP

list dlur lu

Use el mandato **list dlur lu** para visualizar una lista de PU en sentido directo activas (o internas, para TN3270) con estadísticas de LU para cada PU. Las PU dependientes de esta lista tienen un enlace activo con el direccionador o el direccionador actualmente está intentando establecer un enlace.

Ejemplo:

```
APPN >1i dlur lu
CP NAME                LINK      TOTAL  ---NO SSCP LU STATE---  NO OF LUs
                        NAME      LUs    DOWN  PENDING  ACTIVE  LU_LU SESS
-----
STFNET.VLNN105        PUSUD1    253    0     0     253    0
STFNET.VLNN105        PUSUD21   10     0     0     10     0
STFNET.VLNN105        PUSU02    9      0     0     9      0
STFNET.VLNN105        PUSU01    10     0     0     10     0
```

Tabla 57 (Página 1 de 2). Descripción de la salida de list dlur lu

Elemento	Descripción	Valores clave
CP name	Nombre de CP donde reside la LU. Para LU internas de TN3270, nombre de CP del direccionador.	--
Link name	Nombre de estación de enlace configurada o construida dinámicamente para el enlace con la PU dependiente. Este enlace puede ser externo o interno respecto al direccionador.	--
Total LUs	Suma del número de LU en todos los estados SSCP-LU. No es necesario definir estas LU en el direccionador, sino que se definen en el sistema principal.	--

Tabla 57 (Página 2 de 2). Descripción de la salida de list dlur lu

SSCP-LU state: down	Número de LU que no tienen un SSCP propietario pero sí tienen sesiones de LU-LU (enlace SSCP perdido pero ANS=CONT).	--
SSCP-LU state: pending	Número de LU que están esperando una respuesta ACTLU.	--
SSCP-LU state: active	Número de LU que han recibido una respuesta ACTLU. Este número no disminuye cuando se enlaza una LU y entra en el estado LU-LU.	--
LU-LU session	Número de LU que actualmente tienen sesiones de LU-LU activas.	--

list dlur pu

Use el mandato **list dlur pu** para visualizar una lista de PU en sentido directo (o internas, para TN3270) con su estado de conexión. Las PU dependientes de esta lista tienen un enlace activo con el direccionador o el direccionador actualmente está intentando establecer un enlace.

Ejemplo:

```
APPN >li dlur pu
CP NAME          STATUS      LOC LINK      SESS  ANS SSCP      ACT DLUS
                  NAME          NAME          STAT
; PUNAME  NAME
-----
STFNET.VLNN105  active      INT PUSUD1    act   CON PUSUD12  STFNET.MVS8
STFNET.VLNN105  active      INT PUSUD21    act   CON PUSUD1   STFNET.MVS8
STFNET.VLNN105  active      INT PUSU02    act   CON PUSU02   STFNET.MVS8
STFNET.VLNN105  active      INT PUSU01    act   CON PUSU01   STFNET.MVS8
```

Tabla 58 (Página 1 de 2). Descripción de la salida

Elemento	Descripción	Valores clave
CP name	Nombre de CP de la PU dependiente. Para las PU externas, se trata del nombre de CP que envían en el XID o, si no envían ninguno, es un nombre que el direccionador crea utilizando el formato DLUR..@nnn. Para las PU internas, es el nombre de CP del direccionador.	--

Tabla 58 (Página 2 de 2). Descripción de la salida

Status	<p>Estado de la sesión de SSCP-PU, desde la perspectiva del direccionador DLUR.</p> <p>Se pueden decodificar valores de estado del modo siguiente:</p> <ul style="list-style-type: none"> • pe = pendiente • Re = solicitud • Rs = respuesta • Actp, Actpu = ACTPU Dactpu = DACTPU • LnkAct = activación de enlace • Inop = no operativo 	<p>active</p> <p>peReActpRs (por ejemplo, el conducto está inactivo)</p> <p>reset (inactivo)</p> <p>peActpu</p> <p>peActpuRs</p> <p>peLnkAct</p> <p>peDactpuRs</p> <p>peInop</p> <p>peInopActpu</p>
Loc	Ubicación de la PU relativa al direccionador DLUR.	<p>INT = interna</p> <p>DON = en sentido directo</p>
Link name	Nombre de estación de enlace configurada o construida dinámicamente para el enlace con la PU dependiente. Este enlace puede ser externo o interno respecto al direccionador.	--
Sess stat	Estado del conducto DLUR-DLUS que lleva los flujos de control para esta PU dependiente.	<p>act = activo</p> <p>res = restablecer (inactivo)</p> <p>pAct = activo pendiente</p> <p>plnac = inactivo pendiente</p>
ANS	Valor sysdef del sistema principal para la conclusión automática de la red: si las sesiones de LU-LU deben continuar o detenerse cuando se pierde la conectividad SSCP.	<p>CON = continuar</p> <p>STP = detener</p>
SSCP PU name	Nombre de VTAM para esta PU dependiente, recibido en ACTPU.	--
Act DLUS name	Nombre de CP del DLUS que es actualmente propietario de esta PU (el "DLUS activo").	--

list dlur status

Use el mandato **list dlur status** para visualizar un resumen de información de configuración del DLUR global activo actualmente. Tenga en cuenta que algunos de estos valores tienen alteraciones temporales opcionales a nivel de enlace.

Ejemplo:

```

APPN >li dlur st
Primary DLUS Name           = STFNET.MVS8
Backup DLUS Name            =
Retry Time Limit             = 15
Short Retry Timer            = 15
Short Retry Count            = 20
Long Retry Timer             = 30
Drop Link when there are no sessions = NO
    
```

Todos estos elementos de datos están configurados. Consulte la página 127.

list ds incompletes

Use el mandato **list ds inc** para visualizar una lista de solicitudes de búsqueda APPN ("locates") que están en curso actualmente. Este direccionador está esperando respuestas de otros nodos de la red.

El mandato solicita varios filtros de datos posibles. Si desea ver una descripción de cada uno de ellos, consulte la tabla de descripción de la salida que se encuentra a continuación.

Ejemplo:

```

APPN >li ds inc
      PCID (0 if unknown) [00000000 00000000]?
      Locate origin CP      (NetID.CPname or *) [*]?
      Locate origin LU      (NetID.LUname or *) [*]?
      Locate destination LU (NetID.LUname or *) [*]?

PCID & Incomplete
Child CP Name(s)   Origin CP      Origin LU      Destination LU
-----
c49b1f3b 03310d51 STFNET.VLNN105  STFNET.VLNN105  STFNET.VL12
STFNET.VL15

c49b1f3b 03310d50 STFNET.VLNN105  STFNET.VLNN105  STFNET.MVS8
STFNET.VL15
    
```

Tabla 59. Descripción de la salida

Elemento	Descripción	Valores clave
PCID	ID de correlacionador de procedimiento: correlacionador a nivel de red para este procedimiento de búsqueda específico.	--
Incomplete child CP names	Nombres de CP de nodos a los que este direccionador ha enviado solicitudes locate y de los que todavía está esperando respuestas.	--
Origin CP	Nombre del CP que originalmente ha iniciado la búsqueda.	--
Origin LU	Nombre de la LU que originalmente ha iniciado la búsqueda.	--
Destination LU	Nombre de la LU que se está buscando.	--

list ds resource par distintivo-valor

Use este mandato para visualizar una lista de nombres de recursos (LU) del directorio APPN de este direccionador.

Para limitar los datos que se visualizarán, se puede especificar uno de los siguientes distintivos de filtro y un valor correspondiente:

Tabla 60 (Página 1 de 2). Descripción de la salida

Distintivo de filtro	Valor
----------------------	-------

Mandatos de supervisión de APPN

Tabla 60 (Página 2 de 2). Descripción de la salida	
-c	Nombre de CP del propietario de la LU, que puede calificarse con id de red o sin él.
-n	Id de red del propietario de la LU
-l	Nombre de LU completamente calificado
-s	Nombre de servidor completamente calificado

Ejemplo:

APPN >li ds res

```

LU NAME          SERVER NAME      OWNER NAME      LOCATION TYPE
-----
*                STFNET.VLNN105  STFNET.TEMP     WILDCARD HOME
STFNET.MVS8      STFNET.MVS8     STFNET.MVS8     X-DOMAIN CACHE
STFNET.CNM08     STFNET.MVS8     STFNET.MVS8     X-DOMAIN CACHE
STFNET.SD1L02   STFNET.VLNN105  STFNET.VLNN105  LOCAL HOME
STFNET.SD1L03   STFNET.VLNN105  STFNET.VLNN105  LOCAL HOME
STFNET.SD1L04   STFNET.VLNN105  STFNET.VLNN105  LOCAL HOME
  
```

Tabla 61. Descripción de la salida		
Elemento	Descripción	Valores clave
LU name	Nombre de la LU o "*" para representar un comodín total.	--
Server name	Nombre de CP del servidor NN para la LU.	--
Owner name	Nombre de CP del propietario de la LU. Por ejemplo, un EN puede ser propietario de una LU que resida en el EN.	--
Location	Lugar donde está ubicada la LU	REGISTER = registrado por un EN servido X-DOMAIN = dentro o servidor por otro NN LOCAL = en el direccionador, incluyendo LU servidas por DLUR DOMAIN = servido por el direccionador como NN, pero no registrado WILDCARD = el propietario tiene una definición de comodín total (no explícita)
Type	Categoría de entrada del directorio, que refleja cómo debe manejarse la entrada.	HOME = definido por el sistema en el direccionador CACHE = el direccionador la conoce de forma dinámica, caducará REGISTER = registrado por un EN servido, que puede también desregistrarlo

list ds status

Use este mandato para visualizar un resumen de estadísticas acerca del directorio APPN de este direccionador.

Ejemplo:

```
APPN >li ds s
Maximum Directory Entries = 4000
Current Cache Entries    = 3
Current Home Entries     = 284
Registered Entries       = 0
Directed Locates Received = 0
Broadcast Locates Received = 1
Directed Locates Sent    = 2
Broadcast Locates Sent   = 2
Directed Locates Not Found = 0
Broadcast Locates Not Found = 0
Outstanding Locates     = 0
```

list dumps

Use este mandato para listar todos los archivos de vuelco APPN del disco duro del direccionador. Este mandato no está disponible para direccionadores que no tienen disco duro.

Ejemplo:

```
APPN >li du
1      168084      Thu Jul 01 15:11:18 1999
```

Tabla 62. Descripción de la salida

Elemento	Descripción	Valores clave
Number	Número de vuelco a utilizar con el mandato transmit dump	--
Size	Tamaño del archivo de vuelco, en bytes. Este número crece a medida que el vuelco está en curso.	--
Date/time	Fecha y hora de la última modificación de archivo. La hora cambia mientras el vuelco está en curso.	--

list focal

Use este mandato para visualizar una lista de puntos focales de gestión de red dinámica configurados y activos, así como también su estado.

Ejemplo:

```
APPN >li foc
CATEGORY      STATUS  TYPE    FOCAL POINT
-----
ALERT         NOTACT  IMP_PRI STFNET.CNM08
```

Tabla 63 (Página 1 de 2). Descripción de la salida

Elemento	Descripción	Valores clave
Category	Categoría de la función realizada por el punto focal.	ALERT MS_CAPS ACCTNG OTH = otras

Mandatos de supervisión de APPN

Tabla 63 (Página 2 de 2). Descripción de la salida		
Status	Estado de las sesiones LU6.2 respecto a este punto focal.	NOTACT = no activa ACT = activa PENDING NEVERACT = nunca ha estado activa
Type	Naturaleza del punto focal, utilizando términos centrados en el sistema principal: Explícita = El FP no está configurado en el direccionador, se conecta con el direccionador Implícita = El FP está configurado en el direccionador, el direccionador se conecta con el FP Los valores de la derecha se listan en orden de prioridad de mayor a menor, donde un FP de prioridad más alta puede entrar en funciones como FP.	EXP_PRI = primaria explícita IMP_PRI = primaria implícita BKUP_FP = punto focal de seguridad DEF_PRI = primaria por omisión DEF_BKP = copia de seguridad por omisión DOMAIN HOST
Focal point	Nombre de CP del nodo que proporciona la función de punto focal.	--

list isr_sessions Use este mandato para visualizar el número de sesiones de LU-LU ISR activas que pasan por este direccionador, por enlace. La cuenta incluye:

- Sesiones que entran y salen del sistema mediante ISR (estas sesiones cuentan una vez en cada uno de los TG de entrada y de salida)
- Sesiones que entran en el sistema mediante ISR pero salen en una conexión RTP (estas sesiones cuentan una vez sólo en el TG no HPR)
- Sesiones de LU TN3270 direccionadas por DLUR que salen del sistema utilizando ISR (estas sesiones se cuentan sólo en el TG ISR externo real, no en los enlaces internos entre DLUR y las PU locales)

Use el mandato **list session** para visualizar más información acerca de las sesiones ISR que se han contado.

Ejemplo:

```
APPN >li isr
Adjacent CP Name  TG Number  ISR Sessions
=====
STFNET.CP3174BC  21         3
```

Tabla 64 (Página 1 de 2). Descripción de la salida		
Elemento	Descripción	Valores clave
Adjacent CP name	Nombre de CP del nodo adyacente al direccionador de este TG, ya sea configurado o recibido en un XID.	--

Tabla 64 (Página 2 de 2). Descripción de la salida		
TG number	Número de TG negociado para este enlace.	--
ISR sessions	Número de sesiones ISR activas en este enlace.	--

list link_information

Use este mandato para visualizar una lista de todos los enlaces configurados y de todos los enlaces dinámicos activos.

Ejemplo:

```
APPN > li 1
Name      Port Name  Intf      Adj CP Name  Type      HPR      State
-----
T03174    TR005      5         STFNET.CP3174BC  NN  INACTIVE  ACT_LS
TOLEN     TR00       0         STFNET.TEMP     LEN  ENABLED  RESET_LS
TOLEN1    TR00       0         STFNET.ABCD     LEN  ENABLED  RESET_LS
@00      TR005      5         STFNET.NN12     NN   ACTIVE   ACT_LS
```

Tabla 65 (Página 1 de 2). Descripción de la salida		
Elemento	Descripción	Valores clave
Name	Para enlaces configurados, el nombre de estación de enlace que se ha configurado. Para los enlaces dinámicos, el direccionador crea un nombre con el formato "@@nnnn", donde nnnn empieza en cero y continúa aumentando hasta que vuelve a empezar.	--
Port name	Nombre de APPN configurado para el puerto a través del que este enlace está conectado.	--
Intf	Número de interfaz lógica del direccionador para el puerto a través del que este enlace está conectado.	--
Adj CP name	Nombre de CP del nodo adyacente al direccionador en este enlace, ya sea configurado o recibido en un XID.	--
Type	Tipo de nodo configurado o real (si el enlace está activo) del nodo adyacente .	LEN EN NN LEARN (sólo configurado)
HPR	Estado de HPR configurado o real (si el enlace está activo) en el enlace	ACTIVE INACTIVE ENABLED (sólo configurado) DISABLED (sólo configurado)

Tabla 65 (Página 2 de 2). Descripción de la salida

<p>State</p>	<p>Estado de conexión actual del enlace lógico</p> <p>Algunas definiciones de estados intermedios son: SENT_REQ_OPNSTN = el puerto subyacente está activo, se ha pedido a DLC que se ponga en contacto con la estación de enlace remota</p> <p>PEND_XID_EXCH = se ha contactado con la estación remota, se están intercambiando los XID</p>	<p>Estados estables</p> <p>RESET_LS = restablecer (inactivo)</p> <p>ACT_LS = activo (en funcionamiento)</p> <p>Estados de activación</p> <p>SENT_REQ_OPNSTN</p> <p>PEND_XID_EXCH</p> <p>SENT_ACT_AS</p> <p>SENT_SET_MODE</p> <p>SENT_CREATE_TG</p> <p>SENT_CONN_REQ</p> <p>PEND_RCV_CONN_IND</p> <p>PEND_SEND_CONN_RSP</p> <p>SENT_CONN_RSP</p> <p>Estados de desactivación</p> <p>SENT_DEACT_AS_ORD</p> <p>SENT_DISC_ORD</p> <p>SENT_DESTROY_TG</p> <p>PEND_DEACT</p> <p>PEND_CLOSE_STN</p>
--------------	--	---

list link_information nombre-enlace

Use este mandato para obtener información detallada de estado y de configuración de un único enlace lógico con un nodo adyacente.

Ejemplo:

APPN > li link vm30pu1

```

Link Station Information
=====
ls_name = VM30PU1
type = DEFINED
act_at_startup = TRUE
auto_act_supported = FALSE
pan uplink = FALSE
replace inbound CP name/node id = FALSE
retry link act unconditionally = FALSE
adjacent node subnet affiliation = NEGOTIABLE
subnet visit count = 3
remote mac_addr = 402222222222
remote sap_value = 04
hpr_sap_value = C8
real_adj_cp_name = USIBMNR.NRMVM30
node_id = 00000000
cp_cp_sessions_supported = FALSE
hpr_supp = FALSE
hpr_link = FALSE
link station state = ACT_LS
direction = OUTBOUND
actual_max_send_btu_size = 2006
partner_node_type (actual) = EN
partner_node_type (defined) = LEARN
tg_isr_type = ENDPOINT_TG
tg_num (defined) = 0
tg_num (actual) = 0
Received CV22 Sense code = 0
    
```


<i>Tabla 66 (Página 1 de 2). Descripción de la salida</i>		
Elemento	Descripción	Valores clave
Type	Cómo conoce el direccionador al enlace.	DEFINED = configurado DYNAMIC TEMPORARY = todavía no puede coincidir con enlaces configurados
Act_at_startup	Si el enlace está configurado para activarse cuando se inicia APPN.	TRUE FALSE
Auto_act_supported	El enlace puede activarse sólo cuando sea necesario	--
Pan_uplink	Si el enlace está configurado como enlace hacia arriba de Branch Extender (nodo de acceso periférico) (aparición de EN en sentido inverso a NN).	TRUE FALSE
Replace inbound CP name / node ID	Si el enlace está configurado de modo que estos campos de XID de un nodo LEN adyacente deben ser alterados temporalmente por valores configurados en el direccionador.	TRUE FALSE
Retry link act unconditionally	Si la anomalía de activación de enlace y la anomalía de enlace deben volver a intentarse siempre independientemente de la causa.	TRUE FALSE
Adjacent node subnet affiliation	Si el enlace está configurado para ser un enlace EBN con una subred de topología distinta.	NATIVE NON-NATIVE NEGOTIABLE
Real adj CP name	Nombre de CP recibido en un XID del nodo adyacente	--
Sesiones de CP-CP soportadas	Valor configurado desde el puerto del direccionador o definición de enlace	TRUE FALSE
Hpr_supp	Soporte configurado para HPR	TRUE FALSE
Hpr link	Soporte negociado real para HPR en este enlace	TRUE FALSE
Link station state	Estado de conexión actual del enlace lógico	Los mismos valores que en "list link"
Direction	Dirección en la que se ha producido la activación del enlace	INBOUND OUTBOUND
Tg_isr_type	Tipo de TG/Enlace	ENDPOINT_TG = el nodo adyacente actúa como EN INTERMEDIATE_ROUTING_TG = el direccionador actúa como NN o EBN y el nodo adyacente es un NN

Mandatos de supervisión de APPN

Tabla 66 (Página 2 de 2). Descripción de la salida		
Received CV22 sense code	Código de error SNA para una anomalía de intercambio de XID, procedente del nodo adyacente en este enlace.	--

list local_link_information

Use este mandato para visualizar una lista de enlaces lógicos dentro del direccionador desde DLUR a PU2.0 internas. Estas PU se utilizan para contener LU para la función de servidor de TN3270.

Ejemplo:

```
APPN > li loc
Name      SSCP PU Name   Node ID   Auto Act   Sense  State
-----
PUSUD1    STFNET.PUSUD12 77DE711   TRUE       0      LOCAL_ACT_LS
PUSUD21   STFNET.PUSUD1  77D7E11   TRUE       0      LOCAL_ACT_LS
PUSU02    STFNET.PUSU02  77D7F12   TRUE       0      LOCAL_ACT_LS
PUSU01    STFNET.PUSU01  77D7F11   TRUE       0      LOCAL_ACT_LS
```

Tabla 67. Descripción de la salida		
Título de columna	Descripción	Valores clave
Name	Nombre de estación de enlace configurada para el enlace interno con la PU dependiente.	--
SSCP PU name	Nombre de VTAM para esta PU, recibido en la ACTPU.	--
Node ID	Bloque de ID configurado y número de ID para esta PU interna dependiente.	--
Auto act	Si este enlace se activará automáticamente cuando se inicie APPN.	TRUE FALSE
Sense	Código de detección para la última anomalía de enlace.	--
State	Estado actual del enlace lógico interno	Estados estables LOCAL_RESET_LS = restablecer (inactivo) LOCAL_ACT_LS = activo (en funcionamiento) Estados de activación LOCAL_SENT_CREATE_TG LOCAL_SENT_ACT_AS Estados de desactivación LOCAL_SENT_DESTROY_TG LOCAL_PEND_DEACT

list port_information

Use este mandato para visualizar una lista de puertos de direccionador APPN lógicos y físicos configurados, así como también su estado.

Ejemplo:

```

APPN > li port
  Intf      Name      DLC Type      HPR      State
-----
    5      TR005      IBMTRNET      TRUE     ACT_PORT
    0      TR00      IBMTRNET      TRUE     ACT_PORT

```

Tabla 68. Descripción de la salida

Elemento	Descripción	Valores clave
Intf	Número de interfaz lógica del direccionador para este puerto.	--
Name	Nombre de puerto APPN configurado.	--
DLC type	Tipo de interfaz física o configurada.	ATM ETHERAND = ethernet FDDI FR = frame relay HPR_IP = enterprise extender IBMTRNET = red en anillo PPP MPC+ = canal de diversas vías de acceso SDLC X25 = X.25 QLLC
HPR	Estado de HPR por omisión que se ha configurado para los enlaces dinámicos en este puerto.	TRUE FALSE
State	Estado de la interfaz física o lógica tal como APPN lo percibe.	Estados estables RESET_PORT = restablecer (inactivo) ACT_PORT = activo (en funcionamiento) En activación SENT_ENABLE SENT_ACT_SAP En desactivación PEND_START_PORT_DEACT PEND_LS_DEACT_ORD_PORT PEND_LS_DEACT_IMM_PORT SENT_DEACT_SAP

list port_information nombre-puerto

Use este mandato para visualizar información detallada de estado y configuración de un puerto específico.

Ejemplo:

Mandatos de supervisión de APPN

```
APPN > li port t00004
```

```
Port Information
```

```
=====
port_name = T00004
dlc_name = IBMTRNET
port_num = 4
max_rcv_btu_size = 2048
ls_role = NEGOTIABLE
sap_value = 04
mac_addr = 401111111111
hpr_sap_value = C8
pan_uplink = FALSE
adjacent node subnet affiliation = NEGOTIABLE
subnet visit count = 3
hpr_supp = FALSE
port state = ACT_PORT
```

Tabla 69. Descripción de la salida

Elemento	Descripción	Valores clave
DLC name	Tipo de puerto	Los mismos valores que el campo tipo de DLC en "list port"
Port num	Número de interfaz lógica para este puerto port	--
LS role	Función de estación de enlace local inicial en esta interfaz.	PRIMARY SECONDARY NEGOTIABLE
Pan uplink	Si los enlaces dinámicos de este puerto están configurados como enlaces hacia arriba de Branch Extender (nodo de acceso periférico) (aparición de EN en sentido inverso a NN).	TRUE FALSE
Adjacent node subnet affiliation	Si los enlaces dinámicos de este puerto están configurados para ser enlaces EBN con una subred de topología distinta.	NATIVE NON-NATIVE NEGOTIABLE
HPR support	Soporte configurado para HPR en enlaces dinámicos de este puerto	TRUE FALSE
Port state	Estado de la interfaz física o lógica tal como APPN lo percibe	Los mismos valores que en list port

list rtp

Use este mandato para visualizar una lista de entradas en la tabla de asociados RTP y un resumen de información sobre todas las conexiones RTP activas con un punto final en el direccionador (la tabla de conexiones RTP).

La tabla de asociados RTP no aparece si en ella no hay ninguna entrada. Se crea una entrada para cada nodo remoto para el que se dan todas las condiciones siguientes:

- El direccionador ha realizado una configuración de ruta RTP hacia el nodo
- El nodo utiliza sólo un NCE para todas sus conexiones RTP

- El nodo tiene como mínimo una conexión RTP activa con el direccionador

Tenga en cuenta que no se realiza una configuración de ruta RTP durante la activación de RTP de RSETUP o CP-CP, por lo que no habrá ninguna entrada para un nodo adyacente si las únicas conexiones RTP activas con el mismo son para llevar configuraciones de ruta o sesión de CP-CP. Tenga también en cuenta que todos los niveles del IBM 3746-900/950 y los niveles recientes de VTAM utilizan varios NCE.

Ejemplo:

```
APPN > 1i rtp
RTP PARTNER TABLE:
Remote Partner Name Remote Boundary Name TG Number
=====
          STFNET.NN12          STFNET.NN12    -1
          STFNET.VLNN045        STFNET.CP3174BC  21
RTP CONNECTION TABLE:
TCID          CP Name  ISR  APPC  Pathswitch  Alive  COS TPF TG Number
=====
31BE30E0      STFNET.NN12  0    1      180        180   CPSVCMG  21
31BE4428      STFNET.NN12  0    1      180        180   CPSVCMG  21
31BF4850      STFNET.NN12  0    0        0        180   RSETUP   21
31BF5B98      STFNET.NN12  0    1      180        180   SNASVCMG 21
31BF6EE0      STFNET.NN12  0    8      180        180   #CONNECT  21
```

Tabla 70. Tabla de asociados

Elemento	Descripción	Valores clave
Remote partner name	Nombre de CP del nodo en el que una conexión RTP termina.	--
Remote boundary name	Nombre de CP del siguiente nodo ISR adyacente al nodo asociado remoto o nombre de LU de la aplicación remota que utiliza la conexión RTP.	--
TG number	Número del TG que va hacia el siguiente nodo ISR adyacente el nodo asociado remoto. Un valor de "-1" indica que la sesión que ha ocasionado la activación de RTP ha finalizado en el nodo asociado remoto; en este caso el "Remote boundary name" (Nombre de frontera remota) es el nombre de la LU de destino de la sesión en el nodo asociado remoto.	--

Tabla 71 (Página 1 de 2). Tabla de conexiones

Elemento	Descripción	Valores clave
TCID	ID de conexión de transporte, un identificador exclusivo para esta conexión RTP compartido por sus dos puntos finales.	--
CP name	Nombre de CP del nodo en el que esta conexión RTP termina.	--

Mandatos de supervisión de APPN

Tabla 71 (Página 2 de 2). Tabla de conexiones		
ISR	<p>Número de sesiones de LU-LU ISR direccionadas hacia esta conexión RTP del direccionador. Este número incluye los siguientes tipos de sesión:</p> <ul style="list-style-type: none"> • Sesiones desde LU en nodos externos que vienen en ISR y se van en HPR, tanto si se direccionan utilizando DLUR o no • Sesiones desde LU TN3270 en este direccionador que se van en HPR, pero sólo se direccionan utilizando DLUR (las sesiones en enlaces de subárea no pueden utilizar HPR) 	--
APPC	<p>Número de sesiones LU6.2 con un punto final en este direccionador y que se direccionan hacia esta conexión RTP. Este número puede incluir los siguientes tipos de sesión:</p> <ul style="list-style-type: none"> • Sesiones de CP-CP hacia nodos con capacidad para torre CF de HPR • Sesiones de conducto DLUR-DLUS • Sesiones de punto focal • Sesiones de aping 	--
Pathswitch	Tiempo máximo en segundos para realizar una conmutación de recorrido antes de ocasionar una anomalía en la conexión RTP	--
Alive	Tiempo en segundos que ha transcurrido entre mensajes de latido cuando no hay tráfico de usuarios	--
COS TPF	<p>Clase de nombre de servicio para todas las sesiones de esta conexión RTP.</p> <p>Dependiendo de las condiciones de temporización de configuración de la conexión, es normal ver conductos paralelos RTP (con los mismos puntos finales) con la misma clase de servicio.</p>	<p>CPSVCMG = sesiones de CP-CP</p> <p>SNASVCMG = sesiones de DLUR-DLUS o FP</p> <p>#BATCH = prioridad baja estándar</p> <p>#CONNECT = prioridad media estándar</p> <p>#INTER = prioridad alta estándar</p> <p>existen otros nombres creados y definidos por el usuario</p>
TG number	Número de TG/enlace para el primer salto de la conexión RTP fuera del direccionador.	--

list_rtp_tcid

Use este mandato para visualizar información detallada de estado y configuración de una o todas las conexiones RTP.

Ejemplo:

```

APPN > li rtp 31CC5DA8
=====
TCID          CP Name  ISR  APPC  Pathswitch  Alive  COS  TPF  TG  Number
31CC5DA8     STFNET.VL15  0    2      200        180   CPSVCMG  21
RemoteTCID: 00000000 31C680C8, Role: ACTIVE, State: CONNECTED
FwdRSCV: 162B0100 12461080 150BE2E3 C6D5C5E3 *.....STFNET
          4BE503F1 F521                *.VL15.
Xmit:  SentBytes SentFrames  FramesQd  FramesWAck  AllowdRate  ActualRate  Tokens?
      0x00003009 0x00000057      0           0      311Kbps    0Kbps  AVAIL
Recv:  RcvdBytes RcvdFrames  OutOfSeqQ  FramesDiscardd  ARBmode
      0x0000349B 0x00000055      0           0           GREEN
Misc:  SmoothedRoundTrip  SR_timeouts  FramesResent  Pathswitches
      654ms           2           0
;
FwdMinLinkCapacity: 15974Kb/s, ReverseMinLinkCapacity: 15974Kb/s

Each set of data below is taken over 5 min intervals - New(top), Old(bottom)
Allwdsndrate  Actlsendrate  SmRoundTrip  FramesResent  PacketsDisc  GapsReptd
0KB/s         0KB/s         0ms          0             0             0
0KB/s         0KB/s         0ms          0             0             0
0KB/s         0KB/s         0ms          0             0             0
0KB/s         0KB/s         0ms          0             0             0
0KB/s         0KB/s         0ms          0             0             0
0KB/s         0KB/s         0ms          0             0             0
    
```

Tabla 72 (Página 1 de 2). Descripción de la salida

Elemento	Descripción	Valores clave
Role	Función del direccionador en el establecimiento de esta conexión RTP	ACTIVE PASSIVE
State	Estado actual de la conexión. Si la conexión RTP actualmente está experimentando una conmutación de recorrido, se añade la serie "in path switch" al valor del estado (por ejemplo, "CONNECTED, in path switch").	CONNECTED CONNECTING DISCONNECTING OPENED CALLING LISTENING
Tokens?	Si el direccionador tiene permiso para enviar en este instante de tiempo. Es normal que Tokens esté NOT AVAIL cuando FramesQd no es cero, siempre que las visualizaciones subsiguientes muestren SentBytes y SentFrames en aumento.	AVAIL NOT AVAIL
ARB mode	Estado del que el direccionador informa como receptor de su asociado, en base a la congestión de la red detectada mediante cálculos ARB.	GREEN YELLOW RED

Mandatos de supervisión de APPN

<i>Tabla 72 (Página 2 de 2). Descripción de la salida</i>		
SR timeouts	Número de veces que el temporizador Short Request se ha agotado. Este temporizador se inicia cuando el direccionador envía un mensaje de control a su asociado RTP. Si se agota el temporizador, indica que la respuesta no ha llegado dentro del período de tiempo que se esperaba.	--
MinLinkCapacity	Capacidad del TG más lento en esta ruta de RTP.	--
Allowed send rate	Velocidad máxima de envío de datos permitida por el receptor. Se trata de un valor promedio en el intervalo de 5 minutos.	--
Actual send rate	Velocidad de envío de datos calculada en base a los bytes reales que se han transmitido entre las dos últimas solicitudes de velocidad. Si no hay datos para enviar, esta velocidad desciende. Se trata de un valor promedio en el intervalo de 5 minutos.	--
Smoothed round trip	Tiempo medio que se tarda en enviar datos al otro extremo de la conexión y en obtener una respuesta del mismo, en el intervalo de 5 minutos.	
Frames resent	Número de tramas que este direccionador ha enviado en este intervalo de 5 minutos debido a intervalos vacíos de los que ha informado el nodo asociado receptor (un único intervalo vacío puede resultar en el reenvío de varias tramas).	--
Packets disc	Número de paquetes recibidos que este direccionador ha eliminado en este intervalo de 5 minutos, debido a una falta de almacenamientos intermedios APPN en este direccionador o a la detección de una violación del protocolo.	--
Gaps reptd	Número de intervalos vacíos de datos de los que este direccionador ha informado como receptor durante este intervalo de 5 minutos, al nodo asociado que los ha enviado.	--

list session_information

Use este mandato para visualizar una lista de sesiones ISR que fluyen a través del direccionador. Estas sesiones son las

mismas que se han contado por enlace con el mandato **list isr** e incluyen:

- Sesiones que entran y salen del sistema mediante ISR
- Sesiones que entran en el sistema mediante ISR pero salen en una conexión RTP
- Sesiones de LU TN3270 direccionadas por DLUR que salen del sistema utilizando ISR

Este mandato no lista sesiones de control LU6.2 con un punto final en el direccionador; use el mandato **list appc** si desea ver dichas sesiones. Para ver la salida completa de este mandato, debe haber configurado los parámetros de APPN Node Management para guardar la información RSCV para sesiones intermedias.

Ejemplo:

```
APPN > li sess
Origin CP Name      Primary LU      Secondary LU  Mode Name
-----
STFNET.VL15        STFNET.VL15    STFNET.MVS8   #INTER
STFNET.VL15        STFNET.VL15    STFNET.MVS8   SNASVCMG
STFNET.MVS8        STFNET.MVS8    STFNET.VL15   CPSVRMGR
STFNET.VL15        STFNET.VL15    STFNET.MVS8   CPSVRMGR
```

Tabla 73. Descripción de la salida

Elemento	Descripción	Valores clave
Origin CP name	Nombre de CP del nodo propietario de la LU primaria de esta sesión.	--
Primary LU	Nombre de LU de la LU primaria.	--
Secondary LU	Nombre de LU de la LU secundaria.	--
Mode name	Nombre de modalidad que se utiliza para configurar esta sesión. Tenga en cuenta que los nombres de modalidad para las sesiones de control LU6.2 (por ejemplo, conducto DLUR-DLUS) no significan que estas sesiones terminen en el direccionador. Normalmente, pasan a través del direccionador por medio de ISR. Use list appc si desea ver las sesiones que terminan en el direccionador.	#CONNECT = prioridad media normal #INTER = prioridad media alta CPSVCMG = sesión de CP-CP CPSVRMGR = sesión de DLUR-DLUS SNASVCMG = sesión de punto focal otros nombres de modalidad tienen una arquitectura y también pueden ser definidos por el usuario

list status

Use este mandato si desea visualizar un resumen de la información de estado y configuración APPN general. La salida proporciona una visión “rápida” del estado actual.

Ejemplo:

Mandatos de supervisión de APPN

```

APPN > li stat
Fully Qualified CP NAME : STFNET.NETU24
Node up Time           : 6 hrs 50 min 21 Sec
Extended Border Node   : Not Supp   Branch Extender : Not Supp
DLUR                   : ACTIVE     TN3270E       : ACTIVE
Main Mem Stat          : OK         Buffer Mem Stat : OK
    
```

Tabla 74. Descripción de la salida

Elemento	Descripción	Valores clave
FQ CP name	ID de red configurado y nombre de CP de este direccionador.	--
Node up time	Cantidad de tiempo que ha transcurrido desde que se ha reiniciado APPN por última vez.	--
Extended border node	Si el direccionador está configurado para ser un EBN.	Supp = configurado Not Supp = no configurado
Branch Extender	Si el direccionador está configurado para ser un nodo de branch extender.	Supp = configurado Not Supp = no configurado
DLUR	Si la función DLUR está configurada y activa.	ACTIVE = configurada y en funcionamiento NOT ACT = no configurada o no en funcionamiento
TN3270E	Si la función de servidor de TN3270 está configurada y activa.	ACTIVE = configurada y en funcionamiento NOT ACT = no configurada o no en funcionamiento
Main mem stat	Estado actual de la parte principal de la memoria APPN.	OK CONSTRED = restringida CRITICAL
Buffer mem stat	Estado actual de la parte de almacenamiento intermedio de la memoria APPN.	OK SLOWDOWN CONSTRED = restringida CRITICAL

list topo node

Use este mandato para visualizar información de topología de un nodo específico de la subred de topología de este direccionador.

Ejemplo:

```

APPN > li topo node
NODE NAME []? stfnet.rbkim
CP NAME      NODE ROUTE CON TIME  RSN  BN  HPR  ICN  CDS NAT
              TYPE RES  GES  LEFT
;           IVE
=====
STFNET.RBKIM  NN  128  N   15   23   Y  CF   N  N  Y
ACTIVE TGs ORIGINATING FROM THIS NODE

DESTINATION CP  CP_CP  HPR  TG_TYPE  TG NUM
=====
NETIDA.RB61    ACT    Y    APPN    21
STFNET.MVS3    ACT    Y    APPN    21
STFNET.RBBOB   NOTSUP Y    APPN    21
STFNET.RBBRUNO ACT    Y    APPN    21
    
```

<i>Tabla 75 (Página 1 de 2). Descripción de la salida</i>		
Elemento	Descripción	Valores clave
CP name	Nombre de punto de control del nodo de red, que el usuario entrará	--
Node type	Tipo creado del nodo	NN EN VN = nodo virtual (por ejemplo, red de conexión)
Route res	Resistencia a la adición de rutas (más alto significa que es más resistente a la adición de nuevas rutas a través del nodo). Este valor se configura normalmente en el nodo y no es dinámico.	--
Conges	Congestionado o no, tal como el nodo informe de ello dinámicamente.	Y = sí N = no
Time left	Días que faltan para que esta entrada de la base de datos de topología caduque. Si necesita forzar la caducidad de la entrada antes, VTAM proporciona funciones de supresión de topología que pueden hacer que el direccionador elimine entradas.	--
RSN	Número de secuencia de recursos de este nodo, que se utiliza para determinar si una actualización que se ha recibido contiene información nueva que no se ha visto anteriormente.	--
BN	Si el nodo realiza una función de Border Node	Y = sí N = no
HPR sup	Nivel de soporte HPR que el nodo puede realizar	BASE = sólo reenvío de ANR TRAN = transporte - puede tener puntos finales RTP sólo para sesiones de datos CF = flujo de control - puede tener puntos finales RTP para las sesiones de control y de datos
ICN	Nodo de intercambio - si el nodo es VTAM y realiza tanto la función APPN como de subárea SNA	Y = sí N = no
CDS	Servidor de directorio central	Y = sí N = no

Mandatos de supervisión de APPN

Tabla 75 (Página 2 de 2). Descripción de la salida		
Native	Si el nodo está en la subred de topología del direccionador. Tenga en cuenta que un nodo puede tener el mismo id de red y al mismo tiempo estar en una subred de topología distinta.	Y = sí N = no

Si desea obtener una descripción de los campos de la lista "Active TGs originating from this node", consulte **list topo tg**.

list topo status

Use este mandato para visualizar un resumen de estadísticas de la base de datos de topología.

```
APPN > li topo st
Max num of Nodes allowed in Topo( 0 = limit is memory ) : 5400
Current number of Nodes in Topology                   : 25
Number of Node records purged from this node           : 0
Number of TG records purged from this node             : 0
The last flow reduction seq num sent out by this node  : 259
Topology safe store frequency ( 0 = not saved)         : 0
```

Tabla 76. Descripción de la salida		
Elemento	Descripción	Valores clave
Max nodes allowed	Valor calculado del número máximo de nodos permitidos en la base de datos, en base a la cantidad de memoria APPN, el tipo de producto y varios límites mínimos y máximos.	--
Number of node records purged	Número de registros de nodo suprimidos debido a que han caducado o a operaciones de topología de red iniciadas por VTAM.	--
Number of TG records purged	Número de registros de nodo suprimidos debido a que han caducado o a operaciones de topología de red iniciadas por VTAM.	--
Last FRSN sent out	Número de secuencia de reducción de flujo más reciente enviado por este nodo a cualquier otro nodo.	--
Topology safe store frequency	Tiempo configurado en minutos entre copias de seguridad de la base de datos de topología en el disco duro del direccionador.	0 = topology safe store no está habilitado

list topo tg pares distintivo-valor

Use este mandato para visualizar información en la base de datos de topología del direccionador acerca de los TG activos (enlaces o grupos de transmisión) de esta subred de topología.

Para limitar los datos que se visualizarán, se puede especificar uno o más de los siguientes distintivos de filtro y los valores correspondientes.

Tabla 77. Descripción de la salida	
Distintivo de filtro	Valor
-c	Nombre de CP del propietario del TG, que puede calificarse con id de red o sin él.
-n	ID de red del propietario del TG
-p	Nombre plenamente calificado de un asociado de TG

Ejemplo:

```

APPN > 1i topo tg -c c20015
ACTIVE TG's
TG OWNER          TG DESTINATION    CP_CP    HPR  TG_TYPE  TG    RSN
                  NUM
-----
STFNET.C20015     STFNET.VLNN045    ACT      Y    APPN     23    444
STFNET.C20015     STFNET.PDLUR2     ACT      N    APPN      1    436

```

Tabla 78. Descripción de la salida		
Elemento	Descripción	Valores clave
TG owner	Nombre de CP del nodo que ha informado acerca de este TG. Ambos puntos finales de un TG informan acerca del TG, cada uno como propietario con el otro como destino.	--
TG destination	Nombre de CP del otro extremo del TG relativo al propietario.	--
CP-CP	Soporte de sesión de CP-CP en este TG	ACT = activo NOTSUP = no soportado SUPINACT = soportado pero inactivo (por ejemplo, TG paralelos donde sólo uno de ellos puede tener sesiones CP-CP) UNK = desconocido
HPR	Soporte de HPR en este TG	Y = sí N = no
TG type	Tipo creado de este TG	APPN INTER = intercambio, un enlace de subárea a APPN VIRT = virtual; por ejemplo, un enlace a un nodo virtual de red de conexión

Log

Use este mandato para visualizar el registro cronológico de sucesos internos de APPN

Sintaxis:

Mandatos de supervisión de APPN

log

status

view

log status

APPN mantiene su propio registro cronológico de sucesos internos, además del registro cronológico de sucesos ELS del direccionador. Use este mandato para visualizar un resumen de estadísticas actual sobre el registro cronológico de sucesos de APPN.

Ejemplo:

```
APPN > log st
Entries: 32, Discarded: 0, Filtered: 25959, Memory: 9348 of 273400
Filters enabled:
  none
Display direction: Descending
Top Entry:
  32|Jul 23 15:16:15 2F107-24 (E) SCM - UNBIND cleanup is being generated
Bottom Entry:
  1|Jul 23 08:55:45 2F104-14 (E) NOF unable to monitor EGPE environment
Current Time:
  Fri Jul 23 15:47:35 1999
```

Tabla 79. Descripción de la salida

Elemento	Descripción	Valores clave
Entry numbers	Número total de entradas, número de las eliminadas debido a que el registro estaba lleno y número de las filtradas por estar duplicadas.	--
Memory size	Tamaño actual y tamaño máximo del registro de errores en bytes. El tamaño máximo se fija en un 1% aproximado de la memoria APPN.	--
Filters enabled	Lista de filtros de visualización de la salida del registro cronológico que están establecidos actualmente.	none Severity: <i>nivel de gravedad</i> Message: <i>ID de mensaje</i>
Display direction	Orden temporal de visualización de la salida que está establecido actualmente.	Descending (lo más reciente aparece en primer lugar) Ascending
Top/bottom entries	Línea de resumen de cada una de estas entradas (el orden depende de la dirección de visualización). Esto le permite ver el ámbito de tiempo de las entradas actualmente en el registro cronológico.	--
Current time	Día y fecha actuales con la misma base que las entradas del registro cronológico.	--

log view

Use el mandato **log view** para entrar un submenú de mandatos para navegar y ver el registro cronológico de sucesos de APPN.

Cuando entre en la modalidad de visualización del registro cronológico, puede utilizar los mandatos **bottom**, **top**, **goto**, **next**, y **prev** para moverse y visualizar entradas de registro en modalidad de resumen (una página de entradas de 1 ó 2 líneas cada vez). Use los mandatos **det next**, **det prev** y **det entry** para moverse y visualizar detalles de entradas de registro individuales.

El submenú de visualización del registro cronológico también contiene mandatos para controlar los valores para la visualización del registro cronológico. Se puede utilizar el mandato **filter** para seleccionar el nivel mínimo de gravedad que desea ver o para buscar sólo un único tipo de mensaje. Cada uso del mandato **filter** altera temporalmente todos los valores anteriores; no combina con los mandatos anteriores. Se puede utilizar el mandato **set** para establecer las preferencias de visualización del registro cronológico.

La sintaxis y las funciones del submenú son las siguientes:

<i>Tabla 80 (Página 1 de 2). Sintaxis del submenú de Log view</i>		
Mandato	Palabras clave y parámetros	Función
<u>b</u> ottom		Mover al final, mostrar página de resumen
<u>c</u> urrent		Volver a visualizar la página de resumen actual
<u>d</u> etail	<u>n</u> ext_entry	Visualizar la siguiente entrada detalladamente
	<u>p</u> rev_entry	Visualizar la entrada anterior detalladamente
	<u>e</u> ntry_id <i>seq_num</i>	Visualizar la entrada especificada detalladamente
<u>f</u> ilter	<u>a</u> ll	Borrar los filtros de salida (mostrar todo)
	<u>o</u> nly <u>s</u> everity <u>a</u> ction_required	Mostrar las entradas de esta gravedad o mayor.
	<u>c</u> ritical	
	<u>e</u> rror	
	<u>w</u> arning	
	<u>i</u> nformational	
	<u>m</u> essage <i>id-mensaje</i>	Mostrar sólo las entradas con este mensaje
<u>g</u> oto_entry	<u>s</u> equence_num	Mover a la entrada, mostrar página de resumen
<u>n</u> ext_page		Visualizar la página de resumen siguiente
<u>p</u> rev_page		Visualizar la página de resumen anterior
<u>s</u> et	<u>l</u> ines_in_page	Mostrar esta cantidad de líneas en la página
	<u>d</u> irection <u>a</u> scending	Mostrar la entrada más reciente en último lugar

Mandatos de supervisión de APPN

Tabla 80 (Página 2 de 2). Sintaxis del submenú de Log view		
	<u>d</u> escending	Mostrar la entrada más reciente en último lugar
<u>t</u> op		Mover al principio, visualizar página de resumen
<u>e</u> xit		Volver al menú principal de APPN t 5

Ejemplo:

```

APPN > log v
LOG VIEW
LOG VIEW >?
BOTTOM
CURRENT
DETAIL
FILTER
GOTO_ENTRY
NEXT_PAGE
PREV_PAGE
SET
TOP
EXIT
LOG VIEW > top
32|Jul 23 15:16:15 2F107-24 (E) SCM - UNBIND cleanup is being generated
31|Jul 23 15:16:15 2F107-24 (E) SCM - UNBIND cleanup is being generated
30|Jul 23 15:08:15 2F10A-1A (I) Request Route
29|Jul 23 15:08:15 2F10A-07 (E) REQUEST_ROUTE_RSP failed
28|Jul 23 15:08:15 2F10A-1A (I) Request Route
27|Jul 23 15:08:15 2F10A-07 (E) REQUEST_ROUTE_RSP failed
26|Jul 23 15:08:15 2F10A-1A (I) Request Route
25|Jul 23 15:08:15 2F10A-07 (E) REQUEST_ROUTE_RSP failed
24|Jul 23 11:41:06 2F120-18 (C) Correlation table entry was not found.
23|Jul 23 11:37:46 2F120-18 (C) Correlation table entry was not found.
22|Jul 23 11:07:27 2F120-18 (C) Correlation table entry was not found.
21|Jul 23 11:07:27 2F126-0D (E) TNS0013I %1: Keepalive processing detected error
; the connection between IP addr %2 and LU %3 has been ended.

LOG VIEW > det e 21
-----
Sequence Number: 210
APPN Lifetime: 7206.950 seconds
Fri Jul 23 11:07:27 1999
ProbeID 226066B3
Message 2F126000-0000000D
Severity: Error

TNS0013I %1: Keepalive processing detected error ; the connection between IP addr
%2 and LU %3 has been ended.
(Sn) e124102
(Sn) 15.170.99.210
(Sn) STAT1

```

Tabla 81 (Página 1 de 2). Descripción de la salida (Página de resumen, de izquierda a derecha)		
Elemento	Descripción	Valores clave

Tabla 81 (Página 2 de 2). Descripción de la salida (Página de resumen, de izquierda a derecha)

Sequence number	Número exclusivo que se asigna a este suceso cuando se escribe en el registro cronológico (no cuando se visualiza). Es el número que se utiliza con los mandatos "goto" y "detail".	--
Date / time	Momento en que el suceso se ha producido, de acuerdo con el reloj de este direccionador.	--
Message ID	Identificador de mensaje de mayor a menor para la condición que se ha producido. Consulte "APPN Log Event Reference Guide" si desea obtener una descripción de cada mensaje posible. Añada tres ceros a la parte mayor y reste seis ceros a la parte menor del ID para correlacionarlo con los valores de la Reference Guide.	--
Severity	Clasificación APPN de la gravedad del suceso. Los valores clave se listan por orden de gravedad descendiente.	A = es necesario realizar alguna acción C = grave E = error W = aviso I = informativo
Event name	Breve descripción del suceso. Use el mandato "detail" y la Reference Guide si desea obtener más información.	--

Tabla 82 (Página 1 de 2). Descripción de la salida (Detalles del suceso)

Elemento	Descripción	Valores clave
Sequence number	El mismo número que se ha descrito anteriormente para la página de resumen.	--
APPN lifetime	Tiempo en segundos desde que se inició APPN por última vez.	--
Date / time	Igual que en la página de resumen.	--

Mandatos de supervisión de APPN

<i>Tabla 82 (Página 2 de 2). Descripción de la salida (Detalles del suceso)</i>		
Probe ID	ID para la ubicación exacta del software que ha registrado este error.	
Message ID	Igual que en la página de resumen, pero ampliado con ceros iniciales o finales para coincidir con la "APPN Log Event Reference Guide".	--
Severity	Los mismos valores que en la página de resumen, pero expandidos en palabras.	Ver el anterior
Event name	Breve descripción del suceso, ampliado por los elementos de datos que se listan debajo del mismo. Use la Reference Guide si desea obtener más información.	--
Data type labels	Identificadores para los distintos tipos de datos registrados con cada mensaje. Consulte la Reference Guide si desea ver una descripción de los elementos de datos de cada mensaje.	(Ix) (Se) (X) otros ...

Memory

Use el mandato **Memory** para visualizar información sobre el uso de la memoria de APPN.

Sintaxis:

memory

Ejemplo:

```
APPN > mem
```

```
APPN memory status:
```

	Size (MB)	Percent in-use	State
Main	152	17	OK
Buffer	19	0	OK
Total	171	14	

```
APPN total shared memory size= 179200000, special use= 800
APPN main part: size = 159487200 crit_thresh= 151512840 cons_thresh= 143538480
APPN main part: inuse= 26516176 (incl: Trace tbl=65536, Error log= 1447)
APPN main part: peak memory usage= 26518048
APPN main part: event counts: crit= 0 cons= 0 OK = 1
APPN main part: OK for last 278211 seconds
APPN bufr part: size = 19712000 crit= 18726400 cons= 17740800 slow= 13404160
APPN bufr part: inuse= 1232 reserved (< slow)= 24992
APPN bufr part: peak memory usage= 26360
APPN bufr part: event counts: crit= 0 cons= 0 slow= 0 OK = 1
APPN bufr part: OK for last 278211 seconds
```

Tabla 83 (Página 1 de 2). Descripción de la salida

Elemento	Descripción	Valores clave
Total shared memory	<p>Tamaño configurado de la memoria de datos del servidor de TN3270 y APPN, en bytes. Se establece al configurar APPN. No incluye el espacio del código de direccionador o APPN, ni la memoria de almacenamiento intermedio/datos necesaria para otros componentes del direccionador.</p> <p>La parte de "uso especial" no cuenta en la parte principal (main part) o en las partes de almacenamiento intermedio (buffer parts) y es para estructuras de control de sistemas APPN.</p>	--
Main part	<p>Parte de la memoria compartida APPN que se utiliza para bloques de control, tablas de rastreo, mensajes internos y otros datos dinámicos y fijos generales.</p> <p>Esta parte incluye dos áreas de datos especiales: - una tabla de rastreo (Trace tbl) que se fija en el 2% de la memoria compartida total o 64KB, el valor que sea mayor. Para Network Utility, se fija en 20MB. Esta tabla se asigna durante el arranque de APPN. - un registro de sucesos (registro cronológico de errores) que crece hasta un 1% de la memoria compartida total</p>	--
Buffer part	<p>Parte de la memoria compartida de APPN que se utiliza para el almacenamiento intermedio de tramas/paquetes.</p> <p>La parte "reservada" de la misma es un número dinámico de espacio de almacenamiento intermedio comprometido que estadísticamente sirve para a un espacio de almacenamiento intermedio lógico mayor. "< slow)" indica que este valor debe permanecer por debajo del umbral lento para un funcionamiento normal.</p>	--

Mandatos de supervisión de APPN

<i>Tabla 83 (Página 2 de 2). Descripción de la salida</i>		
Main states	<p>Estado de la parte principal de la memoria APPN en relación a valores de umbral calculados.</p> <p>Cuando el estado principal se va congestionando progresivamente, APPN efectúa algunas de estas acciones para ayudar a disminuir la congestión: poner como ocupados los enlaces locales y rechazar búsquedas de difusión entrantes.</p>	<p>OK</p> <p>Constrained</p> <p>Critical</p>
Buffer states	<p>Estado de la parte del almacenamiento intermedio de la memoria APPN en relación a los valores de umbral calculados. Tenga en cuenta que el estado del almacenamiento intermedio se considera grave en cualquier momento en que el de la parte principal sea grave, independientemente del nivel de uso de memoria de almacenamiento intermedio.</p> <p>Cuando el estado del almacenamiento intermedio se va congestionando progresivamente, APPN efectúa algunas de estas acciones para facilitar la disminución de la congestión: rechazar nuevas sesiones, aminorar el flujo de datos de la sesión, informar de que el nodo está congestionado en las actualizaciones de la topología, desacelerar los remitentes de RTP, poner como ocupados los enlaces locales e incluso desconectar las sesiones actuales de prioridad más baja.</p>	<p>OK</p> <p>Slowdown</p> <p>Constrained</p> <p>Critical</p>
Inuse, peak usage	Número actual de bytes en uso y marca máxima que el valor en uso ha alcanzado.	--
Event counts	Número de veces que se ha producido un estado específico desde que APPN se ha reiniciado por última vez.	--
<state> for last nn seconds	Tiempo que la parte de la memoria ha estado en el estado actual. Si el nodo ha entrado alguna vez en un estado de agotamiento, se proporciona información adicional acerca de la duración del estado, tiempo que ha transcurrido desde que se produjo, etc.	--

Rtp status

Use el mandato **rtp status** para visualizar información de la configuración de RTP global actualmente en uso.

Sintaxis:

rtp status

Ejemplo:

```
APPN > rtp stat
Network          High      Medium    &
nbspc; Low
Liveness timer   180      180      180      180
Path Switch Timer 180      180      180      180
Retries          6        6        6        6
```

Tabla 84. Descripción de la salida

Elemento	Descripción
Network, etc.	Prioridad de transmisión SNA
Liveness timer	Tiempo en segundos que transcurre entre mensajes de latido cuando no hay tráfico de usuarios.
Path switch timer	Tiempo máximo en segundos para realizar una conmutación de recorrido antes de ocasionar una anomalía en la conexión RTP.
Retries	Número de reintentos de solicitud breve que se pueden efectuar antes de intentar realizar una conmutación de recorrido.

Rtp switchpath

Use el mandato **rtp switchpath** para forzar una conmutación de recorrido HPR por una conexión RTP que tiene un punto final en este direccionador. La operación de conmutación de recorrido selecciona el mejor recorrido disponible actualmente, que en realidad puede ser el actual. En cualquier caso, la conmutación de recorrido ocasiona una suspensión temporal del flujo del tráfico de usuario en la conexión RTP especificada.

Para utilizar este mandato, en primer lugar use **list rtp** para determinar el TCID de la conexión RTP sobre la que desee forzar la conmutación de un recorrido. Escriba "rtp switch" y proporcione dicho TCID cuando se le solicite. Para ver el resultado de la conmutación de recorrido, use **list rtp tcid** y mire el estado de la conexión para determinar el momento en que la conmutación de recorrido se ha completado (el estado cambia a "activo"). Se puede ver el nuevo recorrido en el RSCV o con la utilización de **rtp test**.

Sintaxis:

rtp switchpath

Rtp test

Use el mandato **rtp test** para realizar una prueba de ruta HPR y visualizar información de cada salto de enlace del recorrido de la conexión RTP. Use primero el mandato **list rtp** para determinar el TCID de la conexión RTP que desee probar. Este mandato realiza la misma acción que el antiguo mandato **test rtp**

Sintaxis:

rtp test

Ejemplo:

```
APPN > rtp test
Enter TCID of the route to be tested [0]? 31B96928
Route Test issued
Waiting for 10 Seconds.....
Information
=====
Result      : SUCCESS
Detailed Information
=====
TG OWNER          TG DEST NAME          TGNUM  RT    DELTA  RESULT
                   TIME    TIME
=====
STFNET.VLNN105    STFNET.VL16           21     8     8      SUCCESS
STFNET.VL16       STFNET.VL15           21    68    60      SUCCESS
```

Tabla 85. Descripción de la salida

Elemento	Descripción	Valores clave
Result (overall)	Estado o motivo de la anomalía de la operación de prueba de ruta.	SUCCESS IN PROGRESS NO RESPONSE INVALID NCE ID INVALID TCID NO ROUTE
TG owner	Nombre de CP del nodo más próximo de este salto de ruta.	--
TG dest name	Nombre de CP del nodo más lejano de este salto de ruta.	--
TG num	Número para este enlace tal como se negocia entre el propietario y el destino.	--
RT time	Tiempo total en milisegundos desde el direccionador hasta el destino del TG.	--
Delta time	Tiempo total en milisegundos desde el propietario del TG al destino, es decir, la parte de tiempo RT que es sólo para este salto.	--
Result (detailed)	Estado de alcance del destino de este salto.	SUCCESS NO RESPONSE

Restart

Use el mandato **restart** para reiniciar APPN y TN3270 con una interrupción, sin reiniciar ni volver a cargar el resto del software del direccionador. Si APPN todavía no se ha detenido, este mandato detiene APPN antes de reiniciar.

Cuando se reinicia APPN, utiliza la información de configuración que está actualmente en memoria, tanto si dicha información se ha escrito en disco mediante el mandato de `talk 6 write` (sólo para modelos de direccionador con disco duro).

Sintaxis:

restart

Stop

Use el mandato **stop** para detener APPN y TN3270 con una interrupción y sin afectar al resto de la ruta.

Sintaxis:

stop

TN3270E

Use el mandato **tn3270e** para acceder al indicador de mandatos TN3270E> desde el que podrá visualizar información sobre la configuración de TN3270E.

Consulte la Tabla 86 si desea ver una descripción de estos mandatos.

Sintaxis:

tn3270e

Mandatos de supervisión de TN3270E

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte la sección "Cómo obtener ayuda" en la página xxix.
Deactivate <i>nombre_lu</i>	Desactiva una LU en uso por parte de un cliente de TN3270 y también puede desconectar la correspondiente conexión TCP con ese cliente.

Tabla 86 (Página 2 de 2). Resumen de los mandatos de supervisión de TN3270E

Mandato	Función
List	<p>Lista los elementos siguientes de la memoria de configuración:</p> <ul style="list-style-type: none"> • Connections • Connections <i>nombre LU</i> • Connections <i>dirección IP</i> • Maps • Pools • Pools <i>nombre agrupación</i> • Ports • Status
Exit	<p>Le devuelve al nivel de mandatos anterior. Consulte la sección “Cómo salir de un entorno de nivel inferior” en la página xxix.</p>

Deactivate LU

Use el mandato **deactivate LU** para desactivar una LU que está en uso por parte de un cliente de TN3270 y para desconectar la conexión TCP correspondiente con ese cliente. Use primero el mandato **list conn** para determinar el nombre de la LU local en base a la dirección IP, nombre de LU de VTAM o nombre de agrupación.

Este mandato proporciona un estado de conclusión satisfactorio/anómalo y también se pueden utilizar los mandatos list para comprobar el estado. Después de la desactivación, el cliente ya no debe aparecer más bajo **list conn**, y el *nombrepu* de **list lu** o **list pu** debe reflejar el cambio del estado de la LU.

Sintaxis:

deactivate lu *nombre_lu local*

List

Use el mandato **list** para visualizar información sobre conexiones TN32870.

Sintaxis:

list
connections
lu *nombre_LU_interna*
mapping
pools
pools *nombre_agrupación*
ports
pu
pu *nombre_pu*

rejections

status

Mandato Función

list connections par *distintivo-valor*

Use este mandato para visualizar una lista completa o de subconjunto de las conexiones de cliente de TN3270 activas.

Para limitar los datos que se visualizarán, se puede especificar uno o más de los siguientes distintivos de filtro y los valores correspondientes:

Distintivo de filtro	Valor
-l (el distintivo no es necesario, simplemente puede escribir el valor)	Nombre de LU del direccionador o nombre de agrupación
-i (el distintivo no es necesario, simplemente puede escribir el valor)	Dirección IP de cliente o una subserie dominante de dicha dirección. Por ejemplo, 9.67 satisfará a todas las direcciones IP del formato 9.67.*.*
-p	Nombre de LU primaria de VTAM
-s	Nombre de LU secundaria de VTAM (normalmente no coincide con el nombre de LU del direccionador)

Ejemplo:

```
TN3270E > li conn
Local LU  Class  Assoc LU  Client Addr  Status  Prim LU  Sec LU  Idle Min
-----
PU1LU207  IW           9.37.182.187  LU-LU  NRAVM30  LU22207  8
PU1LU60   IW           9.37.176.39   LU-LU  NRAVM30  LU2260   52
PU1LU89   IW           9.37.178.49   LU-LU  NRAVM30  LU2289   288
```

Título de columna	Descripción	Valores clave
Local LU	Nombre de LU configurada o definida por el sistema principal en el direccionador.	--
Class	Tipo de LU	IW = estación de trabajo implícita EW = estación de trabajo explícita IP = impresora implícita EP = impresora explícita
Assoc LU	Para una LU de estación de trabajo, nombre de cualquier LU de impresora asociada	--
Client addr	Dirección IP del cliente. Tenga en cuenta que una única dirección IP de cliente puede tener varias LU en uso, variando el puerto TCP de origen.	--

Tabla 88 (Página 2 de 2). Descripción de la salida		
Status	Estado conectado de la LU	SSCP-LU state LU-LU state blank = la conexión TCP existe pero la LU todavía no está conectada
Prim LU	Nombre de LU primaria tal como VTAM la conoce	--
Sec LU	Nombre de LU secundaria tal como VTAM la conoce	--
Idle min	Número de minutos desde que esta conexión ha tenido algún dato de usuario	--

list lu nombre LU interna

Use este mandato para visualizar información de estado y de configuración detallada sobre una única LU interna. Use los mandatos **list conn** o **list pu nombre** para ayudar a determinar el nombre de LU del direccionador para una LU específica.

Ejemplo:

```

TN3270E > li lu pu1lu207
LUNAME : PU1LU207      NAU : 207          LINK NAME : VM30PU1
POOL NAME : PUBLIC     MODEL : 3270002
SSCP_LU ST: NOT PCHSCON , LUENABLE , NOT ACTLURSP , NOT TRMNOTFY
              NOT NOTIFIED , ACTIVATD , NOT DEACTNG , NOT ACTVING
              NOT NMVTSNT , NOT NMVTRCV , COUNTED , NOT DACPUPEN
              NOT TERMPEND , NOT NMVTOFF
LU_LU ST : NOT SNTUNBD , BOUND , NOT UNBINDING , NOT BINDING
FLAGS : NOT SEGFOR , FAPBP , GETPCID , NOT BINDFRT
              NOT SESSTOP , NOT DETCHRCV , LSACON , HSACON
FLAGS1 : NOT MUEXPD , NOT PENDSF , WRAPNORM , NOT INOPST
              NOT SLI , NOT EXIT , OWNED , INITCOMP
VERB FLAGS: NOT EXIT , NOT SF , NOT TERM , NOT INIT , NOT PURG , NOT RD1
              NOT RD2 , NOT RD3 , NOT RD4 , BID , NOT WR1 , NOT WR2
ACTLU : 4915          DACTLU : 0          BIND : 0
UNBIND : 0           NOTIFY : 1
MINI TRACE WRAPPED : NO NUMBER OF ENTRIES : 7
OTHERS : 14 : INIT ,NEW : INIT ,GETPCID : INIT ,PCIDREPY: INIT ,PCHSCOND
INIT ,SENNOTFY: INIT ,NOTFYRSP

```

Tabla 89 (Página 1 de 2). Descripción de la salida		
Título de columna	Descripción	Valores clave
LU name	Nombre de LU configurada o definida por el sistema principal en el direccionador, que el usuario entrará.	--
NAU	Dirección NAU de 1 byte SNA de esta LU en la PU (2-254). Este valor ahora se visualiza en decimal.	--
Link name	Para enlaces de sistema principal de subárea, nombre de estación de enlace del enlace externo asociado con esta PU. Para enlaces de sistema principal de DLUR, nombre de estación/PU del enlace interno con DLUR.	--

<i>Tabla 89 (Página 2 de 2). Descripción de la salida</i>		
Pool name	Nombre de la agrupación a través de la que un cliente puede seleccionar esta LU.	--
Model	Modelo de impresora o pantalla 3270 a la que esta LU da soporte.	--
SSCP_LU state	Decodificaciones de valor de bits sueltos del estado de sesión de SSCP-LU para esta LU, para uso de ingeniería	--
LU_LU state	Decodificaciones de valor de bits sueltos del estado de sesión de LU-LU para esta LU, para uso de ingeniería	--
Flags, Flags1, Verb flags	Otros distintivos de estado para uso de ingeniería	--
Other output	Demás información de estado para uso de ingeniería use	--

list mapping

Use este mandato para ver las correlaciones configuradas actualmente activas entre una dirección IP de cliente y las LU de TN3270 del direccionador. También se puede probar qué entradas de correlación son aplicables a una dirección IP de cliente específica.

Para limitar los datos que se visualizan a las entradas que el servidor utilizará para una dirección IP específica, simplemente especifique dicha dirección IP cuando invoque este mandato.

Ejemplo:

```
TN3270E > li map
TN3270E Client IP Address to LU Name Maps
Client IP      Address      Resource      Last
Address        Mask         Name          Port  Map  Type  Resource
-----
8.1.1.99      255.255.255.255 <DEFLT>    23   Y   POOL  WORKSTATION
9.9.9.9       255.255.255.255 LU45      0    Y   LU    WORKSTATION
9.1.1.1       255.255.255.255 LU47      0    Y   LU    PRINTER
4.4.4.4       255.255.255.255 LU46      0    Y   LU    WORKSTATION
7.7.7.7       255.255.255.255 LU48      0    Y   LU    PRINTER
2.2.2.2       255.255.0.0     POOL2     0    N   POOL  PRINTER
1.1.1.1       1.1.1.1         POOL1     0    N   POOL  WORKSTATION
0.0.0.0       0.0.0.0         <DEFLT>   0    N   POOL  WORKSTATION
```

<i>Tabla 90 (Página 1 de 2). Descripción de la salida</i>		
Elemento	Descripción	Valores clave
Client IP address	Germen de la dirección IP para la coincidencia de direcciones IP de cliente.	--
Address mask	Máscara de bits que se aplicará al germen de dirección y a direcciones de cliente entrantes para determinar si esta correlación es aplicable a este cliente. Sólo se comparan posiciones de bits donde el bit de máscara es 1.	255.255.255.255 = comparar la dirección IP de cliente entrante completa

<i>Tabla 90 (Página 2 de 2). Descripción de la salida</i>		
Resource name	Nombre de LU o nombre de agrupación configurados en el direccionador	<DEFLT> = agrupación por omisión configurada globalmente
Port	Puerto TCP de destino del servidor para conexiones entrantes que deberá coincidir con esta entrada.	0 = la entrada es aplicable a todos los puertos de destino
Last map	Si se encuentra una coincidencia en esta entrada pero la agrupación/LU no la puede satisfacer o si el servidor debe continuar intentándolo y hacer coincidir la conexión con entradas menos específicas.	Y = sí N = no
Type	Si el nombre del recurso es una LU o una agrupación	LU POOL
Resource	Tipo de LU o tipos de LU en la agrupación	WORKSTATION PRINTER

list pools

Use este mandato para listar agrupaciones nombradas configuradas de LU implícitas. Los clientes pueden solicitar cualquier LU de una agrupación pasando el nombre de agrupación en la solicitud de conexión.

Ejemplo:

```
TN3270E > li pool
```

```
TN3270E Implicit pools
Default pool name : PUBLIC
Name              Class
-----
PUBLIC            WORKSTATION
POOL2             PRINTER
POOL1             WORKSTATION
POOL3             WORKSTATION
POOL4             WORKSTATION
```

<i>Tabla 91. Descripción de la salida</i>		
Elemento	Descripción	Valores clave
Default pool name	Nombre de la agrupación global por omisión donde van todas las LU implícitas no ubicadas en otra agrupación. Esta es la agrupación a la que se hace referencia con la serie <DEFLT> en diversos mandatos y visualizaciones.	--
Name	Nombre configurado de la agrupación	--
Class	Tipo de LU configurado en la agrupación	WORKSTATION PRINTER

list pools nombreagrupación

Use este mandato para mostrar información de configuración detallada de una única agrupación de LU. Este mandato

permite ver cómo se distribuyen las LU de la agrupación entre las PU dependientes, cómo se nombran y qué tipo tienen. Si desea obtener información completa sobre las LU que se encuentran bajo una PU específica, utilice el mandato **list pu nombre**.

Ejemplo:

```
TN3270E >li pools pool1
TN3270E Implicit Pool
-----
Pool Name : POOL1                               Pool Class : WORKSTATION
  Station Name : PU1
    LU Name Mask : @02LU
    Number of lus :200
    Model Type : 3270 mod 2
```

Ejemplo:

```
TN3270E >li pools pool2
TN3270E Implicit Pool
-----
Pool Name : POOL2                               Pool Class : PRINTER
  Station Name : PU1
    LU Name Mask : @03LU
    LU Address Range : 5-10,78-99
    Model Type : SCS

  Station Name : PU1
    LU Name: LU48
    NAU Address : 48
    Model Type : 3270
```

Tabla 92 (Página 1 de 2). Descripción de la salida

Elemento	Descripción	Valores clave
Station name	Para enlaces de sistema principal de subárea, nombre de estación de enlace asociado con la PU dependiente. Para la conexión de sistema principal de DLUR, el nombre de PU local.	--
LU name mask	Sólo para LU implícitas, germen del nombre configurado que el direccionador utiliza para generar nombres de LU en el número o rango de direcciones proporcionado.	--
LU address range	Sólo para LU implícitas, rango de direcciones NAU que el direccionador utiliza para generar LU en esta agrupación bajo esta PU.	--
Number of LUs	Sólo para LU implícitas, número de LU que el direccionador genera bajo esta PU.	--
LU name	Sólo para una única LU explícita, el nombre de LU configurada.	--
NAU address	Sólo para una única LU explícita, la dirección NAU de 1 byte para la LU.	--

Tabla 92 (Página 2 de 2). Descripción de la salida

Model type	Tipo configurado de una única LU o grupo de LU.	Para pantallas: 3270 mod 2 3270 mod 3 3270 mod 4 3270 mod 5 Para impresoras: 3270 SCS
------------	---	--

list ports

Use este mandato para visualizar todos los puertos TCP a los que los clientes TN3270 pueden conectarse y las características configuradas de cada puerto.

Ejemplo:

```

TN3270E > li ports
TN3270E Server Ports
Port Number  TN3270E  Resource Name  Disable Filtering
-----
23           Y          <DEFLT>       N
45           Y          <DEFLT>       N
66           Y          <DEFLT>       Y
88           Y          POOL1         N
99           Y          <DEFLT>       N
  
```

Tabla 93. Descripción de la salida

Elemento	Descripción	Valores clave
Port number	Número de puerto TCP de destino en el direccionador al que se conectan los clientes.	--
TN3270E	Si este puerto se configura para dar soporte a clientes "E" o no.	Y = sí N = no
Resource name	Nombre de agrupación configurado para los clientes que se conectan a este puerto.	<DEFLT> = agrupación implícita por omisión global otros nombres son configurados por el usuario
Disable filtering	Si deben comprobarse las correlaciones de la dirección IP de cliente para los clientes que se conectan a ese puerto.	Y = sí N = no

list pu

Use este mandato para visualizar todas las PU dependientes internas configuradas para las LU de TN3270, incluyendo las que utilizan DLUR y las que utilizan enlaces de sistema principal de subárea.

Ejemplo:

```

TN3270E > li pu
PU NAME      STATUS      NODE ID  TOTAL  DDDLUs  -----LU  IN-----
              LUs      ENABLED  ACTIV  OW
NED AVAILABL
-----
VM30PU1     ACTPU_RCVD  07711111  249    N        249      5      244
VM30PU2     ACTPU_RCVD  07722222  249    N        249      5      244
  
```

Tabla 94. Descripción de la salida

Título de columna	Descripción	Valores clave
PU name	Para las PU asociadas con enlaces de subárea, el nombre de estación de enlace configurada del enlace del sistema principal. Para las PU asociadas con DLUR, el nombre de la PU local configurada.	--
Status	Estado actual de la sesión de SSCP-PU	ACTPU_RCVD NOT ACTIVE
Node ID	ID de nodo interno configurado que representa a esta PU dependiente ante VTAM.	--
Total LUs	Número actual de LU definidas en el direccionador bajo esta PU. Esto incluye tanto las LU configuradas como las LU dinámicas iniciadas por el sistema principal activas.	--
DDDLU enabled	Si esta PU está configurada para la definición de LU dinámica.	Y = sí N = n
LUs active	Número de LU que han recibido una respuesta ACTLU desde el sistema principal. Este número puede incluir tanto las LU de DDDLU iniciadas por el sistema principal como las configuradas.	--
LUs owned	Número de LU que están asociadas con conexiones TCP de cliente.	--
LUs available	Número de LU que están activas o tienen capacidad para DDDLU y no tienen propietario, por lo que están disponibles para ser utilizadas por los clientes de TN3270. Este número puede incluir LU configuradas cuya PU esté activa y dé soporte a DDDLU, pero no incluye LU de DDDLU iniciadas por el sistema principal a menos que estén activas.	--

list pu nombre-pu Use este mandato para visualizar información de configuración y estado de todas las LU bajo una PU dependiente específica del direccionador. Estas LU incluyen:

- LU implícitas configuradas, cuyos nombres el direccionador genera en base a gémenes de nombre configurados y cuyas direcciones NAU el direccionador asigna en base a números configurados de LU o rangos de direcciones
- LU explícitas configuradas, cuyos nombres y direcciones NAU son configurados totalmente

- LU dinámicas iniciadas por el sistema principal, cuyos nombres y direcciones NAU están establecidos por el sistema principal

Ejemplo:

```

TN3270E > li pu vm30pu1
PU NAME      STATUS      NODE ID  TOTAL  DDDL  -----LUs  IN-----
              LUs      ENABLED  ACTIV  OW
NED AVAILABL
-----
VM30PU1      ACTPU_RCVD  07711111 249    N      249      5      249
-----
LU NAME      NAU  STATUS  OWN  POOL  SSCP_LU  LU_LU  FLAGS  FLAGS1
              ADD                                STATUS  STATUS
-----
PU1LU2      02  ACTIV  NO   PUBLIC (04,20) 00      02     00
PU1LU3      03  ACTIV  NO   PUBLIC (04,20) 00      02     00
PU1LU4      04  ACTIV  NO   PUBLIC (04,20) 00      02     00
PU1LU5      05  ACTIV  NO   PUBLIC (04,20) 00      02     00
PU1LU6      06  ACTIV  NO   PUBLIC (04,20) 00      02     00
PU1LU7      07  ACTIV  NO   PUBLIC (04,20) 00      02     00

```

Tabla 95. Descripción de la salida

Elemento	Descripción	Valores clave
LU Name	Nombre de la LU tal como el direccionador la conoce. Este nombre es totalmente configurado en el direccionador, generado por el direccionador en base a un valor de germen configurado o se ha pasado desde el sistema principal para una LU dinámica iniciada por el sistema principal.	--
NAU add	Dirección SNA de 1 byte para esta LU que está bajo esta PU. Este valor se configura en el direccionador, seleccionado por el direccionador, o se pasa desde el sistema principal. El valor ahora se visualiza en decimal.	--
Status	Estado actual de esta única LU	ACTIV NOT ACT
Own	Si esta LU está asociada con una conexión TCP de cliente de TN3270	YES NO
Pool name	Nombre de agrupación a través del que se puede asignar esta LU a un cliente.	En blanco para LU explícitas
SSCP_LU status, LU_LU status, Flags, flags1	Valores hexadecimales de los campos de estado para uso de ingeniería. Para ver estos valores decodificados, use el mandato list lu nombre .	--

list rejections

Use este mandato para visualizar una lista de hasta 99 de las conexiones de cliente de TN3270 rechazadas más recientemente. Esto puede ayudar a ver y corregir el motivo de los rechazos. La lista se ordena con el rechazo más reciente en la

parte superior y muestra todos los rechazos incluyendo los intentos varios por parte del mismo cliente.

Ejemplo:

```
TN3270E > li rej
Connection Rejection Table
-----
1 Time   : 7/23/1999 11:09:00
  Client : 15.170.99.210
  Reason : Client is not authorized by Filter entries
2 Time   : 7/23/1999 11:08:59
  Client : 15.170.99.210
  Reason : Client is not authorized by Filter entries
3 Time   : 7/23/1999 11:08:59
  Client : 15.170.99.32
  Reason : Client is not authorized by Filter entries
```

<i>Tabla 96. Descripción de la salida</i>		
Elemento	Descripción	Valores clave
Time	Día y hora en que se ha producido el rechazo.	--
Client	Dirección IP del cliente.	--
Reason	Texto que describe el motivo por el que el servidor ha rechazado la conexión de cliente. Hay actualmente más de 40 motivos definidos.	Algunos motivos de ejemplo incluyen: El nodo está terminando No se ha podido obtener memoria No hay LU disponibles La LU solicitada no se ha encontrado/no está disponible La validación del tipo de LU ha sido anómala Valor de limitación de LU alcanzado Agrupación de LU agotada La memoria APPN está restringida

list status

Use este mandato para visualizar un resumen de la configuración e información del estado actual de la función de servidor de TN3270.

Ejemplo:

```
TN3270E > li st
TN3270E Server Status Summary

TN3270E IP Address: 9.37.179.142
NetDisp Advisor Port Number: 10008
Keepalive type: NOP           Frequency: 60
Automatic Logoff: N
Client IP Address mapping : N
Number of connections           : 10
Number of available LUA LU's   : 498
Number of LUA LU's pending termination : 0
Number of defined LU's        : 498
Number of connections in SSCP-LU state : 0
Number of connections in LU-LU state  : 10
```

<i>Tabla 97 (Página 1 de 3). Descripción de la salida</i>		
Elemento	Descripción	Valores clave

Tabla 97 (Página 2 de 3). Descripción de la salida

IP address	Dirección IP dentro del direccionador a la que los clientes de TN3270 se conectan	--
NetDisp advisor port number	Número de puerto TCP al que la función de equilibrio de carga de Network Dispatcher puede conectarse para sondear y conseguir información de carga de este servidor.	--
Keepalive type	Si el servidor sondea a los clientes para ver si todavía están activos y cómo lo hace.	None = el servidor no sondea a los clientes y descubrirá la ausencia de un cliente sólo al intentar enviar datos. NOP = el servidor sondea a los clientes al nivel de TCP Timing mark = el servidor sondea a los clientes al nivel de TN3270
Frequency	Intervalo en segundos entre sondeos keepalive	--
Automatic logoff	Si el servidor desconecta a los clientes después de un periodo de inactividad (cuando no hay datos fluyendo en ninguna dirección) o no lo hace.	Y = sí N = no
Client IP address mapping	Si el servidor está habilitado globalmente para correlacionar direcciones IP entrantes con nombres de agrupación/LU	Y = sí N = no
Number of connections	Número actual de conexiones TCP activas con clientes de TN3270	--
Number of available LUA LUs	Número de LU que se activan actualmente desde el sistema principal o que tienen capacidad dinámica de activación. Esto incluye LU que están actualmente en uso por parte de clientes de TN3270.	--
Number of LUA LU's pending termination	Número de LU que se están desactivando y el direccionador está esperando confirmación del sistema principal. Estas LU ya no están asociadas con conexiones de cliente de TN3270.	--
Number of defined LU's	Número de LU que se configuran en el direccionador o LU dinámicas activas iniciadas por el sistema principal.	--

Tabla 97 (Página 3 de 3). Descripción de la salida

Number of connections in SSCP-LU state	Número de conexiones TCP activas asociadas con una LU en estado SSCP-LU. Cuando la LU asociada con una conexión es enlazada por una aplicación y entra en estado LU-LU, este número disminuye (aunque la conexión SSCP-LU todavía esté activa).	--
Number of connections in LU-LU state	Número de conexiones TCP activas asociadas con una LU en estado LU-LU.	--

Soporte de reconfiguración dinámica de APPN

Esta sección describe la reconfiguración dinámica (DR) en la medida en que afecta a los mandatos de Talk 6 y Talk 5.

Delete Interface de CONFIG (Talk 6)(Suprimir interfaz)

APPN da soporte al mandato **delete interface** de CONFIG (Talk 6), teniendo en cuenta lo siguiente:

- Cuando se suprime una interfaz, los puertos y enlaces definidos en esta interfaz se suprimen al reiniciar APPN.
- Si se emite **activate_new_config** de Talk 6 o **restart** de Talk 5 antes de volver a cargar el dispositivo, cualquiera de las interfaces mayores que la interfaz que se ha suprimido no se redefinirá satisfactoriamente.

Activate Interface de GWCON (Talk 5)(Activar interfaz)

APPN da soporte al mandato **activate interface** de GWCON (Talk 5), teniendo en cuenta lo siguiente:

Quando se activa una interfaz, los puertos y enlaces en la SRAM de APPN para esta interfaz se definen al nodo APPN y se activan.

Todos los mandatos específicos de la interfaz de APPN están soportados por el mandato **activate interface** de GWCON (Talk 5).

Reset Interface de GWCON (Talk 5)(Restablecer interfaz)

APPN da soporte al mandato **reset interface** de GWCON (Talk 5), teniendo en cuenta lo siguiente:

- Cuando se restablece una interfaz, los puertos y enlaces definidos en esta interfaz se desactivan. Si se trata de un enlace TN3270E de subárea, se reiniciará el nodo APPN. Para un puerto normal, se suprimen las definiciones de puerto y enlace. Después de que la interfaz se active de nuevo, las definiciones de puertos y de enlaces de vuelven a definir y activar.

Todos los mandatos específicos de la interfaz de APPN están soportados por el mandato **reset interface** de GWCON (Talk 5).

Mandatos Component Reset de GWCON (Talk 5)(Restablecer componente)

APPN da soporte a los siguientes mandatos **reset** de GWCON (Talk 5) específicos de APPN:

Mandato GWCON, Protocol Appn, Restart

Descripción: Este mandato reinicia el nodo APPN.

Efecto en la red: Se interrumpirá el flujo de datos de APPN a través de este nodo. Se detiene y reinicia APPN.

Limitaciones:

También se reflejarán los cambios efectuados a la configuración de APPN (Talk 6).

El mandato **GWCON, protocol appn, restart** da soporte a todos los mandatos de APPN.

Mandatos Activate de CONFIG (Talk 6)(Activar)

APPN da soporte a los siguientes mandatos **activate** de CONFIG (Talk 6):

Mandato CONFIG, Protocol APPN, Activate_new_config (O) mandato CONFIG, Protocol APPN, TN3270E, Activate_new_config

Descripción: Este mandato activa los cambios efectuados en la configuración de APPN.

Efecto en la red: Si el cambio no puede activarse dinámicamente, se reinicia APPN.

Limitaciones:

- Si el cambio no puede activarse dinámicamente, se reinicia APPN. Algunos ejemplos son los cambios efectuados en cualquiera de los parámetros de nodo, los parámetros de DLUR por omisión o los parámetros de tn3270e globales. Algunos de los mandatos de supresión también reinician el nodo APPN. La supresión de puertos o estaciones de enlace no reinicia el nodo APPN excepto si las estaciones de enlace son enlaces tn3270e de subárea.
- Si los cambios se realizan en los parámetros de ajuste, es necesario volver a cargar o reiniciar el dispositivo.

El mandato **CONFIG, protocol appn, activate_new_config (O) CONFIG, protocol appn, tn3270e, activate_new_config** da soporte a todos los mandatos APPN.

Uso de AppleTalk Phase 2

Este capítulo describe los mandatos de configuración de AppleTalk Phase 2 (AP2) e incluye las secciones siguientes:

- “Procedimientos de configuración básicos”
- “Filtros de zona de AppleTalk 2” en la página 287
- “Ejemplos de procedimientos de configuración” en la página 288

Procedimientos de configuración básicos

Esta sección indica los pasos iniciales necesarios para activar el protocolo AppleTalk Phase 2 y ejecutarlo. La información sobre cómo efectuar más cambios de configuración se cubre en las secciones de mandatos del presente capítulo. Para que los cambios de configuración nuevos entren en vigor, deberá reiniciarse el direccionador.

Habilitación de parámetros del direccionador

Cuando configure un direccionador para que reenvíe paquetes de AppleTalk Phase 2, deberá habilitar algunos parámetros sin tener en cuenta el número o tipo de interfaces del direccionador. Si varios direccionadores transfieren paquetes de AppleTalk Phase 2, especifique estos parámetros para cada direccionador.

- **Habilitación global de AppleTalk Phase 2:** Para empezar, deberá habilitar globalmente el software de AppleTalk Phase 2 usando el mandato de configuración **enable ap2** del mismo. Si el direccionador muestra un error en este paso, significa que en la carga no hay software de AppleTalk Phase 2. En dicho caso, póngase en contacto con el representante del servicio al cliente.
- **Habilitación de interfaces específicas:** A continuación, deberá habilitar interfaces específicas a través de las que AppleTalk Phase 2 enviará paquetes. Use el mandato **enable interface interface number** para ello.

Nota: Cuando habilite AppleTalk sobre ATM, deberá habilitar también las interfaces de LAN emulada específicas sobre las que AppleTalk enviará paquetes. No debe habilitar AppleTalk sobre la interfaz ATM física. El uso de la palabra “interfaz” en el resto del capítulo se refiere a la interfaz de LAN emulada y no a la interfaz física de ATM.

- **Habilitación de la suma de comprobación:** A continuación, podrá determinar si el direccionador calculará las sumas de comprobación DDP de los paquetes que origine. El software de suma de comprobación no funciona correctamente en algunas implementaciones de AppleTalk Phase 2, por lo que es posible que no desee originar paquetes con sumas de comprobación por cuestiones de compatibilidad con dichas implementaciones. No obstante, por lo general, deseará habilitar la generación de sumas de comprobación. Se comprobará la suma de comprobación de cualquier paquete reenviado con una.

Establecimiento de los parámetros de red

También debe especificar algunos parámetros por cada red e interfaz que envíe y reciba paquetes de AppleTalk Phase 2. Después de especificar los parámetros, use el mandato de listado de la configuración de AppleTalk Phase 2 para ver los resultados de ésta.

- Establezca el rango de red para los direccionadores de germinación: La coordinación de los rangos de red y las listas de zonas para todos los direccionadores de una red se simplifica designando direccionadores específicos como direccionadores de germinación. Los direccionadores de germinación se configuran con el rango de red y la lista de zonas, mientras que a los otros direccionadores se les dan valores nulos. Los valores nulos indican que el direccionador debe solicitar a la red valores de los direccionadores de germinación. Por cada red (segmento) de cada red de AppleTalk interconectada, debe configurarse, como mínimo, una interfaz de direccionador como direccionador de germinación para la red. Por lo general, en una red hay varios direccionadores de germinación por si falla uno de ellos. Además, un direccionador puede ser direccionador de germinación de algunas o todas las interfaces de red. Use el mandato **set net-range** para asignar el rango de red en los direccionadores de germinación.
- Establezca el número del nodo de inicio: Use el mandato **set node** para asignar el número de nodo de inicio para el direccionador. El direccionador hará AARP para este nodo, pero si ya se está usando, se elegirá un nodo nuevo.
- Añada un nombre de zona: Puede añadir uno o varios nombres de zona por cada red del conjunto de redes. Se puede añadir un nombre de zona para una red determinada en cualquier direccionador conectado a dicha red; no obstante, sólo el direccionador de germinación debe contener la información de nombre de zona para una red conectada. Los direccionadores conectados adquieren dinámicamente el nombre de zona de los direccionadores adyacentes usando el protocolo ZIP. Apple recomienda que, para una red determinada, elija el mismo direccionador de germinación para el número de red y el nombre de zona. El nombre de zona no puede configurarse para una red a menos que el número de red también esté configurado. Para añadir un nombre de zona por cada número de red, use el mandato de configuración **add zone nombre** de AppleTalk Phase 2.

AppleTalk sobre PPP

AppleTalk sobre PPP tiene dos modalidades, de direccionador completo y de semidireccionador. En la primera modalidad, otros direccionadores AppleTalk pueden ver la red punto a punto. En la modalidad de semidireccionador, otros direccionadores no pueden ver la red punto a punto, pero ésta sigue transmitiendo información de direccionamiento de AppleTalk y paquetes de datos.

Para establecer la red en la modalidad de direccionador completo, dé a cada direccionador del enlace PPP un número de red común, un nombre de zona común y un número de nodo único. Si configura un extremo del enlace PPP con un número de red que no sea cero, también deberá configurar dicho extremo para que tenga un número de nodo que no sea cero y para que tenga un nombre de zona. En dicho caso, el otro extremo del enlace debe tener:

- El mismo número de red y nombre de zona y un número de nodo diferente.

- Los números de nodo y red establecidos en cero. El direccionador se informará de dichos números en el direccionador configurado.

Para establecer la red en la modalidad de semidireccionador, configure los dos direccionadores del enlace PPP para que los números de red y de nodo se establezcan en cero y no se use ningún nombre de zona.

Filtros de zona de AppleTalk 2

El filtro de nombres de zona, aunque no sea obligatorio para AppleTalk, es una función muy útil para la seguridad y administración de grandes conjuntos de redes de AppleTalk. Existen también condiciones para restringir el acceso a redes por números de red.

Información general

AppleTalk está estructurado para que todas las redes se puedan identificar de dos maneras. La primera es un número de red o rango de números de red consecutivos que debe ser único en todo el conjunto de redes. El número de red combinado con el número de nodo identifica, de forma única, cualquier estación final del conjunto de redes.

El segundo identificador de la red es uno o varios nombres de zona. Estas series de nombres de zona no son exclusivas en la internet. La estación final se identifica de forma única mediante una serie combinada de **objeto:tipo:serie-ZoneName**.

Un direccionador tiene su primer conocimiento de una red cuando el rango de la red nueva aparece en la actualización de direccionamiento RTMP de un direccionador vecino. A continuación, el direccionador solicita al vecino los nombres de zona de dicha red. Tenga en cuenta que el rango de la red se repite en todas las nuevas actualizaciones de RTMP pero que los nombres de zona sólo se solicitan una vez.

Las estaciones finales obtienen los números de red de los paquetes RTMP de difusión (información de direccionamiento) y, a continuación, eligen un número de nodo. Este par de red/nodo somete a AARP (investigación AARP) para ver si otra estación final ya ha reclamado su uso. Si responde otra estación, la estación final elegirá otro par de red/nodo y el proceso se repetirá hasta que no se reciba ninguna respuesta.

¿Para qué sirven los filtros de nombre de zona?

Cuando la estación final típica de AppleTalk desea usar un servicio (impresora, servidor de archivos) en Apple Internet, primero busca todas las zonas disponibles y selecciona una. A continuación, elige un tipo de servicio y solicita una lista de todos los nombres que notifican el tipo en la zona elegida. Este mecanismo hace que surjan varios problemas.

- Un conjunto de redes grandes puede tener muchas zonas. Puede presentarse al usuario una larga lista para que elija a ciegas las que necesita (y, por lo tanto, inhibiendo la usabilidad de la lista).
- Es posible que el servidor no quiera estar disponible en toda la red (por razones de seguridad). Si el cliente no puede ver la zona en la que está el servicio, aumentará la seguridad.

- Restringir las zonas visibles desde un departamento al resto de las redes permitirá a la administración dejar que el departamento controle (o no) su propio dominio además de no aumentar la actividad general en el resto de las redes (reducción de la administración).

El filtro de los números de red aumenta la seguridad y mejora la administración del conjunto de redes. El filtro de zonas sólo controla el acceso a la red de forma indirecta. Un departamento sin regular puede añadir redes con los mismos nombres de zona pero con números de red nuevos que entren en conflicto con otros departamentos. El filtro de números de red puede usarse para evitar que estas adiciones aleatorias de nombres de zona y de números de red tengan un impacto sobre el resto de la red.

¿Cómo se añaden filtros?

El direccionador se configura con una lista de zonas excluyente (que bloquea las zonas especificadas) o incluyente (permite únicamente las zonas especificadas) para cada dirección de cada interfaz. La interfaz especificada no volverá a anunciar la información de zonas filtrada en la dirección definida. Si se filtran todas las zonas de la lista de zonas de una red, la información de red también se filtrará a través de la interfaz.

- Use los mandatos de configuración **add** y **delete** para crear la lista de filtros para una interfaz.
- Use los mandatos de configuración **enable** y **disable** para especificar cómo se aplica la lista de filtros.

Use mandatos similares para crear filtros de números de red.

Otros mandatos:

Puede usar el mandato AP2 CONFIG> **list** para visualizar toda la información de filtro de las interfaces. Además, el mandato **list** acepta un *núm.interfaz* como argumento para que pueda listar información de una única interfaz.

Ejemplos de procedimientos de configuración

Esta sección trata los pasos necesarios para activar AP2 y ejecutarlo. Para obtener información sobre cómo efectuar más cambios de configuración, consulte “Mandatos de configuración de AppleTalk Phase 2” en la página 293. Para que los cambios de configuración entren en vigor, debe reiniciar el direccionador.

Para acceder al entorno de configuración de AP2, entre **protocol ap2** en el indicador Config>.

Habilitación de AP2

Cuando configure un direccionador para que reenvíe paquetes de AP2, deberá habilitar algunos parámetros. Si varios direccionadores transfieren paquetes de AP2, especifique estos parámetros por cada direccionador. Para habilitar AP2:

1. Use el mandato **enable ap2** para habilitar globalmente AP2 en el direccionador. Por ejemplo:

```
AP2 config>enable ap2
```

2. Habilite las interfaces específicas sobre las que AP2 enviará paquetes. Por ejemplo:

```
AP2 config>enable interface 1
```


Configuración de los parámetros de red

Para establecer el direccionador como direccionador de germinación, debe establecer el rango de red, un número de inicio de nodo y, como mínimo, un nombre de zona. Puede configurar algunas interfaces de un direccionador como direccionadores de germinación y dejar otras como direccionadores sin germinación. Debe tener, como mínimo, un direccionador de germinación por cada red AppleTalk y debe configurar varios direccionadores de germinación en la red por si falla uno de ellos.

Nota: No establezca un rango de red o un número de nodo para semidireccionadores.

1. Use el mandato **set net-range** para establecer el rango de red. Por ejemplo:

```
AP2 config>set net-range
      Interface # [0]? 1
      First Network range number (1-65279, or 0 to delete) []? 1
      Last Network range number (1-165279) []? 5
```

Entre los mismos valores inicial y final para una red con un único número.

2. Use el mandato **set node-number** para establecer el Starting Node Number (número de nodo de inicio) para la interfaz. El direccionador hará AARP para este nodo. Si ya se está usando el número, el direccionador elegirá un número nuevo. Por ejemplo:

```
AP2 config>set node-number
      Interface # [0]? 1
      Node number (1-253, or 0 to delete) []?
1
```

3. Use el mandato **add zone** para añadir uno o varios nombres de zona a la red conectada a la interfaz. Si define un rango de red para una interfaz, también deberá definir los nombres de zonas para la interfaz. Si no ha definido un número de red, no defina nombres de zonas. Por ejemplo:

```
AP2 config>add zone
      Interface # [0]? 1
      Zone name []? Finance
```

Después de especificar los parámetros, puede usar el mandato **list** en el indicador AP2 config> para ver la configuración.

Configuración de filtros de zonas

El filtro de zonas le permite filtrar zonas en las dos direcciones de cada interfaz. Para filtrar los paquetes de entrada, establezca un filtro de entrada. Para filtrar los paquetes de salida, establezca un filtro de salida. La interfaz no volverá a anunciar la información de la zona filtrada en la dirección que defina. Siga los pasos siguientes para establecer un filtro de zona:

1. Añadir filtros de zona a una interfaz. Use el mandato **add zfilter in** para añadir un filtro de zona de entrada a una interfaz. Use el mandato **add zfilter out** para añadir un filtro de zona de salida a una interfaz. Por ejemplo:

```
AP2 config>add zfilter in
      Interface # [0]? 1
      Zone name []? Admin
```

2. Habilite los filtros de zona que ha añadido. Esto activará el filtro y los controles, ya sea el filtro incluyente o excluyente. Los filtros incluyentes sólo reenvían la información de zona en dicho filtro. Los filtros excluyentes sólo bloquean la información de zona de dicho filtro. Por ejemplo:

```
AP2 config>enable zfilter in exc
      Interface # [0]? 1
```

A continuación, se muestran algunos ejemplos que explican cómo establecer filtros de zonas en el conjunto de redes que aparece en la Figura 11 en la página 290.

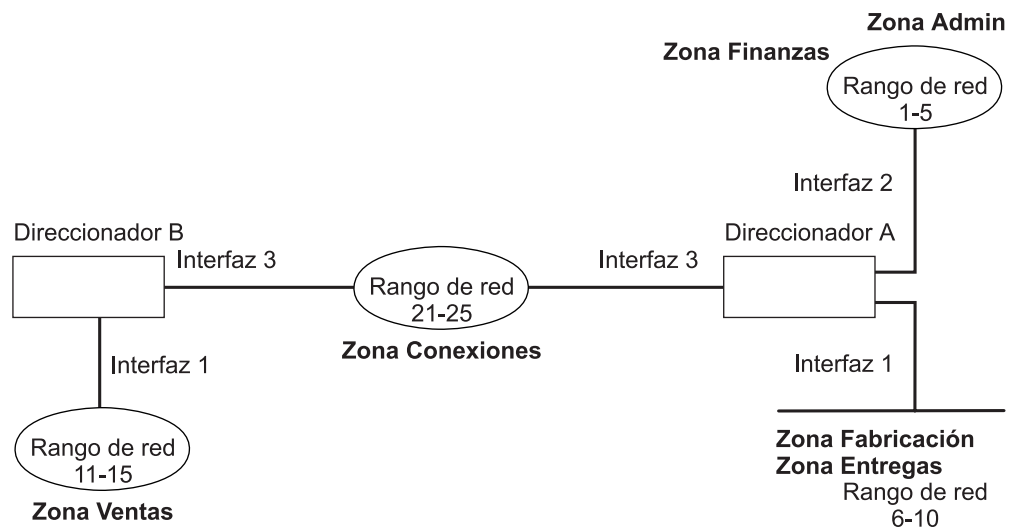


Figura 11. Ejemplo de filtro de zonas

Ejemplo 1

A continuación, se muestra un ejemplo de cómo filtrar la zona de Fabricación en relación con el resto de las redes. Para ello, deberá establecer un filtro de entrada en la interfaz 1 del direccionador A para excluir la zona de fabricación.

1. En el direccionador A, añada un filtro de zonas de entrada para la interfaz 1.

```
AP2 config> add zfilter in
      Interface # [0]? 1
      Zone name []? Manufacturing
```

2. Habilite el filtro de zonas de entrada y conviértalo en excluyente.

```
AP2 config>enable zfilter in exc
      Interface # [0]? 1
```

Esto hará que la zona de fabricación no entre en el direccionador A, por lo que filtrará la zona en relación al resto del conjunto de redes.

Ejemplo 2

El ejemplo siguiente muestra cómo filtrar la zona de fabricación en la red 11-15, pero permitiendo que esta zona se pueda ver en la red 1-5. Para ello, deberá establecer un filtro de salida en la interfaz 3 del direccionador A para evitar que la información de la zona de fabricación se reenvíe fuera de la interfaz 3. La interfaz seguirá anunciando información de la zona de fabricación en las interfaces 1 y 2 del direccionador A, lo que la hará visible en la red 1-5.

1. Añada un filtro de zona de salida a la interfaz 3.

```
AP2 config>add zfilter out
      Interface # [0]? 3
      Zone name []? Fabricación
```

2. Habilite el filtro de las zonas de salida y conviértalo en excluyente.

```
AP2 config>enable zfilter out exc
      Interface # [0]? 3
```

Este filtro excluirá la información de la zona de fabricación de la salida de la interfaz 3.

Ejemplo 3

El ejemplo siguiente muestra cómo establecer un filtro para que la zona de administración sea visible en todas las redes y la zona de finanzas no sea visible en el resto del conjunto de redes.

1. Añada un filtro de zonas de entrada a la interfaz 2 del direccionador A.

```
AP2 config>add zfilter in
Interface # [0]? 2
Zone name []? Admin
```

2. Habilite el filtro de zonas de entrada y conviértalo en incluyente.

```
AP2 config>enable zfilter in inc
Interface # [0]? 2
```

Estableciendo este filtro de entrada como incluyente, sólo se reenviará información de la zona de administración a través de la interfaz 2 al resto del conjunto de redes.

Establecimiento de filtros de red

Los filtros de red son similares a los filtros de zonas, salvo que permiten filtrar toda una red. Para establecer un filtro de red:

1. Añada un filtro de red. Use el mandato **add nfilter in** para añadir un filtro de red de entrada a una interfaz. Use el mandato **add nfilter out** para añadir un filtro de red de salida a una interfaz. Por ejemplo:

```
AP2 config>add nfilter out
Interface # [0]? 2
      First Network range number
(decimal) [0]? 11
      Last Network range number (decimal) [0]? 15
```

El rango de red que entre aquí deberá coincidir con el rango que haya asignado a la red.

2. Habilite el filtro de red que ha añadido y conviértalo en incluyente o excluyente. Los filtros incluyentes sólo reenviarán información de red en dicho filtro. Los filtros excluyentes sólo bloquearán información de red en un filtro y permitirán reenviar el resto de la información de red.

```
AP2 config>enable nfilter in exc
Interface # [0]? 2
```

A continuación, mostramos algunos ejemplos de cómo establecer filtros en el conjunto de redes, tal como se muestra en la Figura 12 en la página 292.

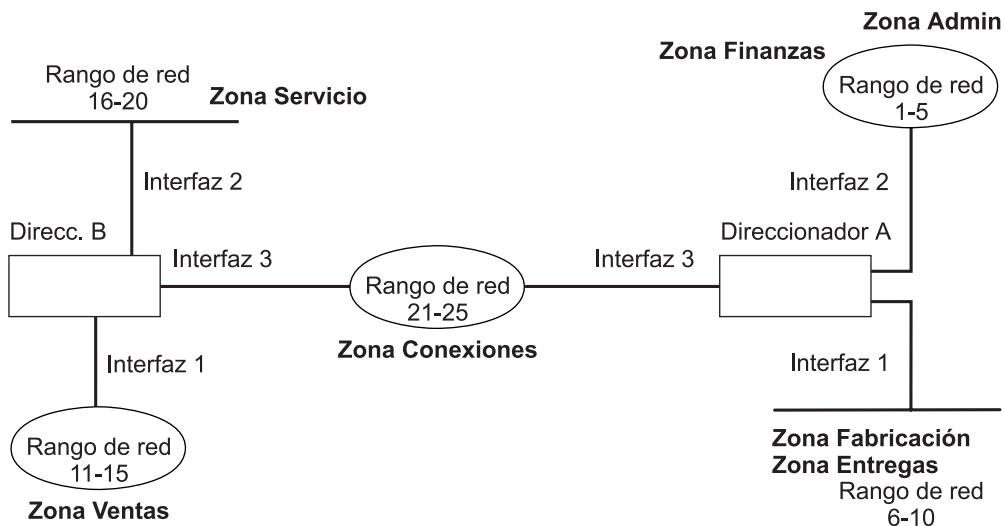


Figura 12. Ejemplo de filtro de red.

Los pasos siguientes muestran cómo filtrar la red 6-10 para que no sea visible a la red 16-20, tal como se muestra en la Figura 12.

1. Añada un filtro de red de salida para la red 6-10 en la interfaz 2 del direccionador B.

```
AP2 config>add nfilter
out
Interface # [0]? 2
First Network range number (decimal) [0]? 6
Last Network range number
(decimal) [0]? 10
```

2. Habilite el filtro de red de salida como excluyente.

```
AP2 config>enable nfilter out exc
Interface # [0]? 2
```

Este filtro evitará que toda la información de la red 6-10 se reenvía a través de la interfaz 2 a la red 16-20.

Configuración y supervisión de AppleTalk Phase 2

Este capítulo describe los mandatos de configuración y supervisión de AppleTalk Phase 2 (AP2). Está formado por las secciones siguientes:

- “Acceso al entorno de configuración de AppleTalk Phase 2”
- “Mandatos de configuración de AppleTalk Phase 2”
- “Acceso al entorno de supervisión de AppleTalk Phase 2” en la página 302
- “Mandatos de supervisión de AppleTalk Phase 2” en la página 302

Acceso al entorno de configuración de AppleTalk Phase 2

Para acceder al entorno de configuración de AppleTalk Phase 2, entre el mandato siguiente en el indicador Config>:

```
Config> ap2
      AP2 Protocol user configuration
      AP2 Config>
```

Mandatos de configuración de AppleTalk Phase 2

Esta sección describe los mandatos de configuración de AppleTalk Phase 2.

Los mandatos de configuración de AppleTalk Phase 2 le permiten especificar parámetros de red para interfaces del direccionador que transmiten paquetes de AppleTalk Phase 2. La información que especifique con dichos mandatos se activará cuando reinicie el direccionador.

Entre los mandatos de configuración de AppleTalk Phase 2 en el indicador AP2 config>. La Tabla 98 muestra los mandatos.

Tabla 98 (Página 1 de 2). Resumen de mandatos de configuración de AppleTalk Phase 2

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte la sección “Cómo obtener ayuda” en la página xxix.
Add	Añade nombres de zona, filtros de red y filtros de zona a una interfaz.
Delete	Suprime los nombres de zona, interfaces, filtros de red y filtros de zona.
Disable	Inhabilita interfaces, sumas de comprobación, direccionamientos de horizonte dividido, filtros de red o filtros de zona o bien inhabilita globalmente AppleTalk Phase 2.
Enable	Habilita interfaces, sumas de comprobación, direccionamientos de horizonte dividido, filtros de red o filtros de zona o bien habilita globalmente AppleTalk Phase 2.
List	Muestra la configuración actual de AppleTalk Phase 2.

Mandatos de configuración de AppleTalk Phase 2 (Talk 6)

Tabla 98 (Página 2 de 2). Resumen de mandatos de configuración de AppleTalk Phase 2

Mandato	Función
Set	Establece el tamaño de la antememoria, el rango de red y el número de nodo.
Exit	Le devuelve al nivel de mandatos anterior. Consulte la sección "Cómo salir de un entorno de nivel inferior" en la página xxix.

Add

Use el mandato **add** para añadir el nombre de zona a la lista de zonas de interfaces o bien para añadirlo a la mencionada lista como valor por omisión para la interfaz o para añadir filtros de red o de zona.

Sintaxis:

```
add          zone . . .  
              defaultzone . . .  
              nfilter in . . .  
              nfilter out . . .  
              zfilter in . . .  
              zfilter out . . .
```

zone *núm.interfaz nombrezona*

Añade el nombre de zona a la lista de zonas de interfaces. Si define un número de red para una interfaz, también debe definir los nombres de zonas para la interfaz. Si no ha definido un número de red, no defina nombres de zonas.

Ejemplo:

```
ap2config>add zone  
Interface # [0]? 0  
Zone name []? Finance
```

defaultzone *núm.interfaz nombrezona*

Añade un nombre de zona por omisión para la interfaz. Si un nodo de la red solicita un nombre de zona que no es válido, el direccionador asignará el nombre de zona por omisión al nodo hasta que se elija otro nombre de zona. Si añade más de un valor por omisión a una interfaz, el último que añada alterará temporalmente el valor por omisión anterior. Si no añade un valor por omisión, el valor por omisión será el primer nombre de zona añadido usando el mandato **zone**.

Ejemplo:

```
ap2config>add defaultzone  
Interface # [0]? 0  
Zone name []? Headquarters
```

nfilter in *núm.interfaz núm.primer red núm.última red*

Añade un filtro de red a la entrada en interfaz. El rango de red que entre debe coincidir con el rango de red que establezca para la interfaz. No puede filtrar únicamente una parte de un rango de red. Por ejemplo, si establece un rango de red de 1–10 y configura un filtro para 5–8, el direccionador filtrará el rango completo de red de 1–10.

Ejemplo:

Mandatos de configuración de AppleTalk Phase 2 (Talk 6)

```
ap2config>add nfilter in
Interface # [0]? 0
First Network range number (decimal) [0]? 1
Last Network range number (decimal) [0]? 10
```

nfilter out *núm.interfaz núm.primera red núm.última red*

Añade un filtro de red a la salida de la interfaz. El rango de red que entre debe coincidir con el rango de red que establezca para la interfaz. No puede filtrar únicamente una parte de un rango de red. Por ejemplo, si establece un rango de red de 1–0 y configura un filtro para 5–8, el direccionador filtrará el rango completo de red de 1–10.

Ejemplo:

```
ap2config>add nfilter out
Interface # [0]? 0
First Network range number (decimal) [0]? 11
Last Network range number (decimal) [0]? 20
```

zfilter in *núm.interfaz nombre zona*

Añade un filtro de nombre de zona a la entrada o salida de la interfaz.

Ejemplo:

```
ap2config>add zfilter in
Interface # [0]? 1
Zone name []? Marketing
```

zfilter out *núm.interfaz nombre zona*

Añade un filtro de nombre de zona a la salida de la interfaz.

Ejemplo:

```
ap2config>add zfilter out
Interface # [0]? 0
Zone name []? Corporate
```

Delete

Use el mandato **delete** para suprimir un nombre de zona de la lista de zonas de interfaces, suprimir filtros de red o de nombre de zona o toda la información de AppleTalk Phase 2 de una interfaz.

Sintaxis:

```
delete           zone . . .
                 nfilter in . . .
                 nfilter ot . . .
                 zfilter in . . .
                 zfilter ot . . .
                 interface
```

zone *núm.interfaz nombrezona*

Suprime un nombre de zona de la lista de zonas de interfaces.

Ejemplo:

```
ap2config>delete zone 2 newyork
```

nfilter in *núm.interfaz núm.primera red núm.última red*

Suprime un filtro de red de la entrada en interfaz. Debe entrar los mismos números de rango de red que ha establecido usando el mandato **add nfilter in**.

Ejemplo:

Mandatos de configuración de AppleTalk Phase 2 (Talk 6)

```
ap2config>delete nfilter in
Interface núm. [0]? 0
First Network range number (decimal) [0]? 1
Last Network range number (decimal) [0]? 12
```

nfilter out *núm.interfaz*

Suprime un filtro de red de la salida de la interfaz. Debe entrar los mismos números de rango de red que ha establecido usando el mandato **add nfilter out**.

Ejemplo:

```
ap2config>delete nfilter out
Interface # [0]? 0
First Network range number (decimal) [0]? 11
Last Network range number (decimal) [0]? 20
```

zfilter in *núm.interfaz nombre zona*

Suprime un filtro de nombre de zona de la entrada en interfaz.

Ejemplo:

```
ap2config>delete nfilter in
Interface # [0]? 1
Zone name []? Marketing
```

zfilter out *núm.interfaz nombre zona*

Suprime un filtro de nombre de zona de la salida de la interfaz.

Ejemplo:

```
delete zfilter out
Interface # [0]? 1
Zone name []? Marketing
```

interface Use este mandato para suprimir una interfaz. Es la única manera de suprimir nombres de zonas que tienen caracteres que no se imprimen.

Ejemplo:

```
ap2config>delete interface 1
```

Disable

Use el mandato **disable** para inhabilitar AP2 en todas las interfaces o en una interfaz especificada, la suma de comprobación, filtros, la conversión APL/AP2 o el direccionamiento de horizonte dividido.

Sintaxis:

```
disable      ap2
               checksum
               interface . . .
               nfilter in . . .
               nfilter out . . .
               zfilter in . . .
               zfilter out . . .
               split-horizon-routing . . .
```

ap2 Inhabilita el reenviador de paquetes de AppleTalk Phase 2 para todas las interfaces.

Ejemplo:

```
ap2config>disable ap2
```

checksum

Especifica que el direccionador no calculará la suma de comprobación en los paquetes que genere. Por lo general, el direccionador efectúa la

Mandatos de configuración de AppleTalk Phase 2 (Talk 6)

suma de comprobación de todos los paquetes que reenvía. Este es el valor por omisión.

Ejemplo:

```
ap2config>disable checksum
```

interface *núm.interfaz*

Inhabilita todas las funciones de AP2 en la interfaz de red especificada. La red sigue estando disponible para el resto de los protocolos.

Ejemplo:

```
ap2config>disable interface 2
```

nfilter in *núm.interfaz*

Inhabilita, pero no suprime, los filtros de red de entrada de esta interfaz.

Ejemplo:

```
ap2config>disable nfilter in
Interface # [0]? 2
```

nfilter out *núm.interfaz*

Inhabilita, pero no suprime, los filtros de red de salida de esta interfaz.

Ejemplo:

```
ap2config>disable nfilter out
Interface # [0]? 2
```

zfilter in *núm.interfaz*

Inhabilita, pero no suprime, los filtros de la zona de entrada de esta interfaz.

Ejemplo:

```
ap2config>disable zfilter in
Interface # [0]? 1
```

zfilter out *núm.interfaz*

Inhabilita, pero no suprime, los filtros de la zona de salida de esta interfaz.

Ejemplo:

```
ap2config>disable zfilter out 0
Interface # [0]? 1
```

split-horizon-routing *núm.interfaz*

Inhabilita el direccionamiento de horizonte dividido de esta interfaz. Sólo debe inhabilitarse el direccionamiento de horizonte dividido en las interfaces de Frame Relay que estén en un eje de una red Frame Relay parcialmente dividida. La inhabilitación del direccionamiento de horizonte dividido hace que todas las tablas de direccionamiento se propaguen en esta interfaz.

Ejemplo:

```
ap2config>disable split-horizon-routing 0
```

Enable

Use el mandato **enable** para habilitar la función de suma de comprobación, habilitar una interfaz especificada, habilitar la función de pasarela de AppleTalk 2 o habilitar globalmente el protocolo AppleTalk Phase 2.

Sintaxis:

```
enable          ap2
```

Mandatos de configuración de AppleTalk Phase 2 (Talk 6)

```
checksum  
interface . . .  
nfilter in . . .  
nfilter out . . .  
split-horizon-routing . . .  
zfilter . . .
```

ap2 Habilita el reenviador de paquetes de AppleTalk Phase 2 para todas las interfaces.

Ejemplo:

```
ap2config>enable ap2
```

checksum

Especifica que el direccionador calculará la suma de comprobación en los paquetes que genere. El direccionador calcula la suma de comprobación de todos los paquetes de AP2 que reenvía.

Ejemplo:

```
ap2config>enable checksum
```

interface *núm.interfaz*

Habilita el direccionador para que envíe paquetes de AppleTalk Phase 2 sobre interfaces específicas.

Ejemplo:

```
ap2config>enable interface 3
```

nfilter in *exclusive o exclusive núm.interfaz*

Habilita los filtros de entrada de la red y controla cómo se aplica el filtro a la interfaz. Inclusive (incluyente) reenvía las coincidencias. Exclusive (excluyente) elimina las coincidencias.

Ejemplo:

```
ap2config>enable filter in inc  
Interface # [0]? 1
```

nfilter out *exclusive o exclusive núm.interfaz*

Habilita los filtros de salida de la red y controla cómo se aplica el filtro a la interfaz. Inclusive (incluyente) reenvía las coincidencias. Exclusive (excluyente) elimina las coincidencias.

Ejemplo:

```
ap2config>enable filter out exec  
Interface # [0]? 1
```

split-horizon-routing *núm. interfaz*

Habilita el direccionamiento de horizonte dividido en la interfaz. El valor por omisión es *enabled*.

Ejemplo:

```
ap2config>enable split-horizon-routing 1
```

zfilter

Habilita los filtros de zona asignados a una interfaz. Debe especificar si el filtro está "in" o "out" y si incluye o excluye. Si incluye, sólo los paquetes que coincidan con el filtro se direccionarán. Si excluye, todos los paquetes que coincidan con el filtro se descartarán.

Ejemplo:

```
ap2config>enable zfilter in inc  
Interface # [0]?
```

Ejemplo:

```
ap2config>enable zfilter out exec
Interface # [0]? 0
```

List

Use el mandato **list** para visualizar la configuración actual de AP2. En el ejemplo, el direccionador es un direccionador de germinación en las interfaces 0 y 1

Nota: El mandato **list** acepta un *núm.interfaz* como argumento.

Sintaxis:

list

Ejemplo:

```
ap2config>list
APL2 globally enabled
Checksumming disabled
Cache size 500
```

List of configured interfaces:

```
Interface      netrange      / node      Zone
0              1000-1000    / 1        "SerialLine"(Def)
Input ZFilters disabled
Input NFilters (inclusive)
Output ZFilters disabled
Output NFilters disabled
Split-horizon-routing enabled
1              10-19        / 52       "EtherTalk", "Sales"(Def)
Input ZFilters disabled
Input NFilters (inclusive)
Output ZFilters disabled
Output NFilters disabled
Split-horizon-routing enabled
2              unseeded net / 0
Input ZFilters disabled
Input NFilters (inclusive)
Output ZFilters disabled
Output NFilters disabled
Split-horizon-routing disabled
```

APL2 globally

Indica si AppleTalk Phase 2 se habilita o inhabilita globalmente.

Checksumming

Indica si se habilita o inhabilita la suma de comprobación.

Cache size

(Tamaño de la antememoria) Número de entradas de antememoria de vía de acceso rápido.

List of configured interfaces

(Lista de interfaces configuradas) Lista cada número de interfaz y su rango de red, número de nodo y nombre o nombres de zona, así como la zona por omisión.

Por cada interfaz también lista si los filtros de zona de entrada y salida y los filtros de red están habilitados o inhabilitados. Si están habilitados, indica si son incluyentes o excluyentes.

Mandatos de configuración de AppleTalk Phase 2 (Talk 6)

Input/output Zfilters

Indica los filtros de zona asignados a una interfaz. Si incluye, sólo los paquetes que coincidan con el filtro se direccionarán. Si excluye, todos los paquetes que coincidan con el filtro se descartarán. Se visualizará el nombre de la zona filtrada. Input (entrada) significa que el filtro se aplica al tráfico que entra en la interfaz. Output (salida) significa que el filtro se aplica al tráfico que sale de la interfaz.

Input/output Nfilters

Indica los filtros de red asignados a una interfaz. Si incluye, sólo los paquetes que coincidan con el filtro se direccionarán. Si excluye, todos los paquetes que coincidan con el filtro se descartarán. Se visualizará el rango de redes filtradas. Input (entrada) significa que el filtro se aplica al tráfico que entra en la interfaz. Output (salida) significa que el filtro se aplica al tráfico que sale de la interfaz.

Split-horizon-routing

Muestra si el direccionamiento de horizonte dividido está habilitado o inhabilitado en cada interfaz.

Set

Use el mandato **set** para definir el tamaño de la antememoria de la vía de acceso rápida o parámetros específicos de AppleTalk Phase 2, incluyendo el rango de red en direccionadores de germinación y el número de nodo.

Sintaxis:

```
set          cache-size . . .  
              net-range . . .  
              node . . .
```

cache-size *valor*

tamaño antememoria corresponde al número total de redes y nodos de AppleTalk que pueden comunicarse simultáneamente a través de este direccionador usando la función de vía de acceso rápida. (Fastpath (vía de acceso rápida) es un método de cálculo previo de cabeceras MAC que sirve para reenviar paquetes con mayor rapidez). El valor por omisión es 500, lo que permite a un máximo de 500 redes y nodos comunicarse simultáneamente a través del direccionador y seguir usando la vía de acceso rápida. Si el número de redes y nodos supera el tamaño de la antememoria, el direccionador seguirá reenviando los paquetes, pero no usará la vía rápida. Los valores válidos del tamaño de la antememoria son: 0 (inhabilitar) de 100 a 10000. Aunque no se recomienda, el establecimiento del tamaño de la antememoria en cero inhabilita la función de vía de acceso rápida y no se usa memoria para la antememoria. Sólo debe cambiar este valor por omisión en el caso de las redes muy grandes. Cada entrada de tamaño de la antememoria usa 36 bytes de memoria.

Ejemplo:

```
ap2config>set cache-size 700
```

net-range *núm.interfaz primernúm. últimonúm.*

Asigna el rango de red de los direccionadores de germinación usando:

- *núm.interfaz* - Designa la interfaz del direccionador sobre la que trabajar.
- *primernúm.* - Asigna el número más bajo del rango de red. Los valores legales están incluidos entre 1 y 65279 (hexadecimal 10xFEFF).
- *últimonúm.* - Establece el número más alto del rango de red. Los valores legales están incluidos entre el *primernúm.* y 65279.

Una red con un único número tiene el primer valor y el último valor iguales. Si el primer valor es cero, se suprimirá el rango de red para la interfaz y convertirá la interfaz con "germinación" en una interfaz "sin germinación". *núm.primer* y *núm.último* están incluidos en el rango de red.

Si establece el primer valor en cero en una interfaz Point-to-Point (PPP) permitirá a dicha interfaz funcionar en la modalidad "half-router" (semidireccionador). En dicha modalidad, ninguno de los dos extremos de la red PPP está configurado con un rango de red o una lista de zonas, lo que reduce la cantidad de configuración necesaria. Los dos direccionadores de una red PPP deben funcionar según la misma modalidad.

Nota: Cuando conecte un 2210 a un IBM 6611 usando una interfaz PPP, establezca el 2210 en la modalidad "semidireccionador", la cual es la *única* modalidad de funcionamiento con soporte de IBM 6611 para comunicaciones AppleTalk sobre una interfaz PPP.

Ejemplo:

```
ap2config>set Net-Range 2 43 45
```

node *núm.interfaz núm.nodo*

Asigna el número de nodo de inicio para el direccionador. El direccionador hará AARP para este nodo, pero si ya se está usando, se elegirá un nodo nuevo. A continuación, explicamos cada uno de los argumentos que se entran después del mandato:

- *núm.interfaz* - Designa la interfaz del direccionador sobre la que trabajar.
- *núm.nodo* - Designa el primer número de nodo intentado. Los valores legales están incluidos entre 1 y 253. Un cero como valor *núm.nodo* suprime el número de nodo de la interfaz y obliga al direccionador a elegir uno de forma aleatoria.

Ejemplo:

```
ap2config>set node 2 2
```

Acceso al entorno de supervisión de AppleTalk Phase 2

Para acceder al entorno de supervisión de AppleTalk Phase 2, entre el mandato siguiente en el indicador + (GWCON):

```
+ protocolo ap2
AP2>
```

Mandatos de supervisión de AppleTalk Phase 2

Esta sección describe los mandatos de supervisión de AppleTalk Phase 2 que le permiten ver los parámetros y estadísticas de las interfaces y redes que transmiten paquetes de AppleTalk Phase 2. Los mandatos de supervisión muestran los valores de configuración de los niveles de paquete, trama y físico. También puede visualizar los valores de los tres niveles de protocolo a la vez.

Entre los mandatos de supervisión de AppleTalk Phase 2 en el indicador AP2>. La Tabla 99 muestra los mandatos.

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte la sección "Cómo obtener ayuda" en la página xxix.
Atecho	Envía solicitudes de eco y espera las respuestas.
Cache	Muestra las entradas de la tabla de antememorias.
Clear Counters	Borra todos los contadores de uso de la antememoria y los de desbordamiento de paquetes.
Counters	Muestra la cuenta de desbordamiento de paquetes AP2 por cada interfaz.
Dump	Muestra el estado actual de la tabla de direccionamientos de todas las redes en internet y sus nombres de zonas asociados.
Interface	Muestra las direcciones actuales de las interfaces.
Exit	Le devuelve al nivel de mandatos anterior. Consulte la sección "Cómo salir de un entorno de nivel inferior" en la página xxix.

Atecho

El mandato **atecho** envía AppleTalk Echo Requests (solicitudes de eco) a un destino especificado y espera la respuesta. Este mandato puede usarse para verificar la conectividad básica de AppleTalk y aislar los problemas de la red AppleTalk.

Sintaxis:

atecho *red_dest nodo_dest*

dest_net Especifica el número de red AppleTalk de destino en decimales. Se trata de un parámetro obligatorio.

dest_node

Especifica el número de nodo AppleTalk de destino en decimales. Se trata de un parámetro obligatorio.

Nota: Para la mayoría de los nodos de AppleTalk, la dirección de red (número de red y número de nodo) se asigna dinámicamente y puede que no esté disponible al instante. No obstante, sigue habiendo varias formas de usar el mandato **atecho** con eficacia:

1. En la mayoría de los casos la dirección de AppleTalk para los nodos del direccionador se configura estáticamente. La conectividad entre los nodos del direccionador es crítica para la conectividad general de la red.
2. Si establece el número de nodo de destino de atecho en 255, puede solicitar todos los nodos del número de red especificado en una red AppleTalk conectada directamente. Las respuestas recibidas indicarán los números de nodo de los nodos. A continuación, podrá usar estos números para ejecutar echo en ellos desde direccionadores distantes a fin de verificar la conectividad.

src_net Número de red AppleTalk de origen. Se trata de un parámetro opcional. Si no se especifica, el direccionador usará su número de red de la interfaz en la interfaz de salida que lleva a la red de destino. Si la interfaz de salida es una interfaz PPP de semidireccionador no numerado, el direccionador usará cualquiera de sus nodos de red de interfaz con la LAN.

src_node Número de nodo AppleTalk de origen. Se trata de un parámetro opcional. Si no se especifica, el direccionador usará su número de nodo de interfaz en la interfaz de salida que lleva a la red de destino. Si la interfaz de salida es una interfaz PPP de semidireccionador no numerado, el direccionador usará cualquiera de sus nodos de red de interfaz con la LAN.

size Número de bytes que deben usarse en las solicitudes de eco de AppleTalk. Se trata de un parámetro opcional. El valor por omisión es 56 bytes.

rate Velocidad de envío de solicitudes de eco de AppleTalk. Se trata de un parámetro opcional. El valor por omisión es un segundo.

Nota: Si entra **atecho** sin parámetros, se le solicitarán el resto de los parámetros. Entre valores para los parámetros obligatorios y entre también valores para los parámetros opcionales o bien acepte los valores por omisión.

Cache

El mandato **cache** muestra información sobre las entradas de tamaño de la antememoria.

Sintaxis:

cache

Ejemplo: cache

Destination	Interface	Usage	Next Hop
122/22	1	1	27/5
138/51	0	1	27/5
23/7	1	1	Direct

Mandatos de supervisión de AppleTalk Phase 2 (Talk 5)

Destination

(Destino) Dirección del nodo de AppleTalk (número de nodo/número de red).

Net (Red) Número de la interfaz usada para reenviar al nodo de destino.

Usage (Uso) Número de veces que esta entrada de la antememoria se ha usado en este período de fijación, que es de cinco segundos. Una entrada no usada se suprimirá después de 10 segundos.

Next Hop (Salto siguiente) La dirección de AppleTalk del direccionador del salto siguiente usado para reenviar un paquete al nodo de destino, o Direct (directo) si el nodo de destino está conectado directamente a la interfaz.

Clear Counters

El mandato `clear-counters` borra todos los contadores de uso de la antememoria y los contadores de desbordamiento de paquetes.

Sintaxis:

`clear-counters`

Counters

Use el mandato `counters` para visualizar el número de desbordamientos de paquetes en cada red que envía y recibe paquetes de AppleTalk Phase 2. Este mandato muestra el número de veces que la cola de entrada del reenviador de AppleTalk Phase 2 estuvo llena cuando se recibieron paquetes de la red especificada.

Sintaxis:

`counters`

Ejemplo: counters

AP2 Input Packet Overflows

Net	Count
FR/0	0
Eth/0	4
PPP/0	22

Dump

Use el mandato `dump` para obtener información de la tabla de direccionamientos sobre las interfaces del direccionador que reenvía paquetes de AppleTalk Phase 2.

Nota: `dump núm.interfaz` muestra la parte de la red general e información de zona que es visible en la interfaz mencionada.

Sintaxis:

`dump`

Ejemplo: `dump`

Mandatos de supervisión de AppleTalk Phase 2 (Talk 5)

Dest Net	Cost	State	Next hop	Zone
10-19	0	Dir	0/0	"Ethertalk", "Sales"
40-49	1	Good	10/13	"Marketing", "CustomerSer", "TokenTalk"
20-29	2	Sspct	10/13	"Fuchsia", "Backbone", "Engineering", "MKTING"

3 entries

También puede usar el mandato **dump** con una interfaz específica para mostrar las ruta visibles en dicha interfaz. Puede usar esta función para asegurarse de que los filtros estén configurados correctamente ya que muestra si las redes o zonas filtradas están visibles en una interfaz.

Ejemplo: dump 0

View for interface 0

Dest net	Cost	State	Next hop	Zone
214-214	1	Good	152/152	"eth-214"
153-153	0	Dir		"eth153"
152-152	0	Dir		"ser152"

3 entries

Dest Net Especifica el número de red de destino en decimales.

Cost Especifica el número de saltos del direccionador a esta red de destino.

State Especifica el estado de la entrada de la tabla de direccionamientos. Incluye lo siguiente:

Next hop Especifica el salto siguiente de los paquetes que van a redes que no están directamente conectadas. Para las redes conectadas directamente, se trata del número de nodo 0.

Zones Especifica el nombre de red comprensible para las personas. Los nombres de zona se ponen entre comillas en caso de que contengan espacios incorporados o caracteres que no se imprimen. Si el nombre de zona contiene caracteres del juego superior al juego de caracteres ASCII de 7 bits (caracteres de 8 bits), el nombre de zona que aparece dependerá de las características del terminal de supervisión.

Interface

Use el mandato **interface** para visualizar las direcciones en todas las interfaces del direccionador en las que esté habilitado AppleTalk Phase 2. Si la interfaz está presente en el direccionador pero está inhabilitada, este mandato mostrará el estado.

Nota: `interface núm.interfaz` muestra el filtro activo de la interfaz. Muestra la red, el nodo, la zona por omisión y los filtros activos de una interfaz.

Sintaxis:

`interface`

Ejemplo: interface

Interface	Addresses
PPP/0	0/1 on net 1000-1000 default zone "SerialLine"
Eth/0	10/52 on net 10-19 default zone "Sales"
PPP/1	0/0 in startup range
TKR/0	0/0 on net 20-29 default zone "Backbone"

Mandatos de supervisión de AppleTalk Phase 2 (Talk 5)

También puede entrar el mandato interface seguido de un número de interfaz específico para ver la configuración de AP2 en dicha interfaz.

Ejemplo: interface 1

```
Eth/0 1/30 on net 1-5 default zone "marketing"
```

```
Input Net filters inclusive 1-5  
Output Zone filters inclusive "finance"  
Output Net filters exclusive 1-5
```

Uso de VINES

Este capítulo describe los mandatos que sirven para configurar el protocolo Banyan VINES e incluye las secciones siguientes:

- “Visión general de VINES”
- “Protocolos de capa de red de VINES” en la página 308
- “Procedimientos de configuración básicos” en la página 315
- “Acceso al entorno de configuración de VINES” en la página 317
- “Ejecución de Banyan VINES en el direccionador de puenteo” en la página 315
- “Mandatos de configuración de VINES” en la página 317.

Nota: Si necesita información más detallada sobre los protocolos de VINES, consulte la publicación de Banyan: *VINES Protocol Definition*, (Definición de protocolos VINES), número de pedido: 003673

Visión general de VINES

VINES sobre protocolos e interfaces de direccionador

El protocolo VINES direcciona paquetes VINES sobre las interfaces y protocolos siguientes:

- PPP Banyan Vines Control Protocol (PPP BVCP)
- Frame Relay
- Ethernet/802.3
- 802.5 Token Ring
- X.25
- Ethernet ATM LAN Emulation Client
- Token-Ring ATM LAN Emulation Client

También da soporte a paquetes en 802.5 Source Routing Bridge (SRB).

El protocolo VINES se implementa en la capa de red (Capa 3) del modelo OSI. VINES direcciona paquetes desde la capa de transporte de un nodo a la de transporte de otro nodo. Como VINES direcciona los paquetes a los nodos de destino de estos, los paquetes pasan a través de las capas de red de los nodos intermedios donde se comprueba si tienen errores de bit. Un paquete VINES IP puede contener un máximo de 1500 bytes, incluyendo la cabecera de la capa de red y todos los datos y cabeceras de los protocolos de las capas superiores.

Nodos cliente y de servicio

La red VINES está formada por nodos de servicio y nodos cliente. Un nodo de servicio proporciona servicios de direccionamiento y de resolución de direcciones a los nodos cliente. Un nodo cliente es un vecino físico de la red VINES. Todos los direccionadores son nodos de servicio. Un nodo Banyan puede ser de servicio o cliente.

Cada nodo de servicio tiene una dirección de red de 32 bits y una de subred de 16 bits. IBM 2210 tiene una dirección de red configurable. Esta dirección identifica al direccionador como nodo de red de servicio para Vines. Banyan ha asignado el rango incluido entre 30800000 y 309FFFFF para que IBM lo use en sus

direccionadores. Este direccionador usa el rango incluido entre 30900000 y 3097FFFF.

Nota: Es muy importante que no se asigne la misma dirección de red a dos direccionadores. La dirección de red de un nodo de servicio de Banyan es el número de serie hexadecimal de 32 bits del nodo de servicio. La dirección de subred de todos los nodos de servicio es 1.

Por lo general, la dirección de red de cada nodo cliente es la dirección de red del nodo de servicio de la misma red. No obstante, si un nodo cliente se encuentra en una LAN que tiene más de un nodo de servicio, se le asignará la dirección de red del nodo de servicio que responda primero a la solicitud de asignación de dirección del nodo cliente. La dirección de subred de cada nodo cliente es un valor hexadecimal incluido entre 8000 y FFFE.

Protocolos de capa de red de VINES

Esta implementación de VINES está formada por los cuatro protocolos de capa de red siguientes. Las secciones siguientes describen estos protocolos y sus implementaciones.

- “VINES Internet Protocol (VINES IP)”. Direcciona paquetes a través de la red.
- “Routing Update Protocol (RTP)” en la página 310. Distribuye información de topología para dar soporte a los servicios de direccionamiento proporcionados por VINES IP.
- “Internet Control Protocol (ICP)” en la página 313. Proporciona funciones de soporte y diagnóstico a algunas entidades de protocolo de la capa de transporte como, por ejemplo, notificar algunos errores de red y condiciones topológicas.
- “VINES Address Resolution Protocol (VINES ARP)” en la página 314. Asigna direcciones de internet de VINES a nodos cliente que todavía no tengan direcciones.

VINES Internet Protocol (VINES IP)

El protocolo VINES IP direcciona paquetes por la red usando el número de red de destino de la cabecera de VINES IP. VINES IP está formado por una cabecera de red de 18 bytes que sirve de prefijo a cada paquete. La Tabla 100 en la página 309 resume los campos contenidos en la cabecera.

Implementación de VINES IP

Cuando VINES IP recibe un paquete, comprueba que no tenga errores de excepción y tamaño. Un error de tamaño es un paquete con menos de 18 bytes o más de 1500 bytes. Si tiene un error de tamaño, VINES IP descartará el paquete. Un error de excepción es, por ejemplo, una suma de comprobación errónea o una cuenta de saltos que haya expirado.

Si el paquete no tiene errores de excepción o de tamaño, VINES IP comprobará la dirección de destino y reenviará el paquete como sigue:

- Si la dirección de destino es la misma que la dirección de VINES IP local y la suma de comprobación es válida, el nodo local aceptará el paquete.
- Si la dirección de destino es la misma que la dirección de reenvío y la suma de comprobación es válida, VINES IP aceptará el paquete, lo procesará

localmente y comprobará el campo de la cuenta de saltos de la cabecera IP. Si la cuenta de saltos es superior a 0, VINES IP la disminuirá en uno y volverá a reenviar el paquete a todos los soportes locales salvo al que recibió el paquete.

- Si la dirección de destino no es la misma que la dirección de VINES IP local o la dirección de difusión, VINES IP consultará las tablas de direccionamiento para saber cuál es el salto siguiente. Si la cuenta de saltos está en 0, VINES IP descartará el paquete. De lo contrario, disminuirá dicha cuenta en uno y reenviará el paquete al salto siguiente.

Si la dirección de VINES IP de destino no está en la tabla de direccionamientos y se ha establecido el bit de error en el campo de control del transporte, VINES IP eliminará el paquete y enviará al origen, un mensaje indicando que es imposible llegar al destino. Si el bit de error del campo de control del transporte no está establecido, VINES IP descartará el paquete y no enviará ningún mensaje al origen.

Tabla 100 (Página 1 de 2). Resumen de los campos de la cabecera de Vines IP

Campo de la cabecera de VINES IP	núm. de bytes	Descripción
Checksum (suma comprob.)	2	Detecta una corrupción de error de bits en el paquete.
Packet Lenght (long. paq.)	2	Indica el número de bytes del paquete, incluyendo los datos y la cabecera de VINES IP.

Tabla 100 (Página 2 de 2). Resumen de los campos de la cabecera de Vines IP

Campo de la cabecera de VINES IP	núm. de bytes	Descripción
Transport Control (contr. trans.)	1	<p>Está formado por los cinco subcampos siguientes:</p> <p>Class (Clase) Determina el tipo de nodos a los que se envían los paquetes de difusión de VINES.</p> <p>Error Si el bit de error está establecido, cuando no se puede direccionar un paquete a un nodo cliente o un nodo de servicio, se envía un paquete de notificación de excepción a la entidad de protocolo de la capa de transporte.</p> <p>Metric (Métrica) Solicita que el nodo de servicio del nodo cliente de destino indique al origen un coste de direccionamiento desde el nodo de servicio al nodo cliente de destino.</p> <p>Redirect (Redireccionar) Indica si el paquete contiene un mensaje RTP que especifica una ruta mejor.</p> <p>Hop Count (Cuenta de saltos) Especifica el rango por el que puede viajar un paquete. El rango de la cuenta de saltos puede estar incluido entre 0x0 y 0xf.</p>
Protocol Type (Tipo prot.)	1	Especifica el protocolo de la capa de red VINES del paquete como VINES IP, RTP, ICP o VINES ARP.
Destination Network Number (Núm. red dest.)	4	Número de red de 4 bytes de la dirección VINES IP del destino.
Destination Subnetwork Number (Núm. subred dest.)	2	Número de subred de 2 bytes de la dirección VINES IP del destino.
Source Network Number (Núm. red origen)	4	Número de red de 4 bytes de la dirección VINES IP de origen.
Source Subnetwork Number (Núm. subred origen)	2	Número de subred de 2 bytes de la dirección VINES IP de origen.

Routing Update Protocol (RTP)

RTP reúne y distribuye información de direccionamiento que VINES IP usa para calcular rutas en toda la red. RTP habilita a cada direccionador para que difunda periódicamente tablas de direccionamiento a todos los vecinos. A continuación, el direccionador determina el vecino de destino que usará para direccionar el paquete.

Los nodos de servicio mantienen dos tablas: una tabla de direccionamientos y otra de vecinos. Ambas tablas tienen temporizadores que dan una antigüedad a su contenido para poder eliminar las entradas que hayan quedado anticuadas. Las actualizaciones de direccionamientos para las interfaces X.25 se efectúan cuando se produce un cambio en la base de datos de direccionamientos, por ejemplo, cuando un nodo se activa o desactiva o cuando se producen cambios métricos.

Tabla de direccionamientos

La tabla de direccionamientos contiene información sobre los nodos de servicio. La Figura 13 muestra una tabla de direccionamientos de ejemplo. Después de la figura, se describen los campos contenidos en la tabla.

Net	Address	Next Hop	Nbr	Addr	Nbr	Intf	Metric	Age (secs)
S	30622222		30622222	:0001		Eth/0	20	30
H	0027AA21		0027AA21	:0001		Eth/1	2	120
P	0034CC11		0034CC11	:0001		X.25/0	45	0
3 Total Routes								
S ⇒ Entry is suspended, H ⇒ Entry is in Hold-down,								
P ⇒ Entry is permanent								

Figura 13. Tabla de direccionamientos de ejemplo

Descripción de campos de la tabla de direccionamientos

Net Address

(Dirección de la red) La dirección de la red es un número de 32 bits único. Si delante del campo de dirección de la red se encuentra una S, una H o una P, los significados serán los siguientes:

- S** Indica que el nodo de servicio está suspendido y se anuncia durante 90 segundos que está desactivado. Después de este tiempo, el direccionador elimina la entrada correspondiente a este nodo de la tabla de direccionamientos.
- H** Indica que el nodo de servicio está retenido y se anuncia durante 2 minutos que está desactivado. Después de este tiempo, el direccionador anunciará que el nodo de servicio está operativo. Si un nodo de servicio está suspendido y recibe un paquete RTP, el nodo de servicio entrará en estado de retención.
- P** Indica que la interfaz X.25 entra en estado permanente durante 4-1/2 minutos después de la inicialización. Después de este tiempo, el vecino entrará en dicho estado y su edad permanecerá en 0 mientras se encuentre así. Si la interfaz X.25 se desactiva, se eliminará la entrada de la tabla de direccionamientos.

Next Hop Nbr Addr

(Dir. vecino salto siguiente) Dirección del nodo de servicio vecino que es el salto siguiente de la vía de acceso de menos costo a la red.

Nbr Intf

(Núm. intf.) El soporte al que el nodo de servicio vecino del salto siguiente está conectado.

Metric

(Métrica) Costo estimado, en incrementos de 200 milisegundos, de direccionar el paquete VINES al nodo de servicio de destino.

Age (secs)

(Edad - secs) Edad actual, en segundos, de la entrada. Si un direccionador no recibe una actualización de un nodo de servicio que está en la tabla de direccionamientos en un período, como mínimo, de 360 segundos (6 minutos), el direccionador eliminará la entrada correspondiente al nodo de servicio de la tabla de direccionamientos.

Tablas de vecinos

La tabla de vecinos contiene información sobre los nodos de servicio vecinos y los nodos clientes conectados al direccionador. La Figura 14 muestra una tabla de vecinos de ejemplo y, después de la figura, se describen los campos contenidos en la tabla.

Nbr	Address	Intf	Metric	Age(secs)	H/W Addr	RIF
30633333:0001	TKR/0	4	30	0000C0095012		
0035CC10:8000	Eth/1	2	120	0000C0078221		
2 Total Neighbors						

Figura 14. Tabla de vecinos de ejemplo

Descripción de campos de la tabla de vecinos

Nbr Address

(Dirección vcn) La dirección del nodo vecino. En la Figura 14, la dirección 30633333:0001 es un nodo de servicio y la dirección 0035CC10:8000 es un nodo cliente.

Intf

(Intf.) El soporte al que está conectado el nodo vecino.

Metric

(Métrica) Costo estimado, en incrementos de 200 milisegundos, de direccionar el paquete VINES al nodo vecino.

Age (secs)

(Edad - secs) Edad actual, en segundos, de la entrada. Si un direccionador no recibe una actualización de direccionamiento de un vecino en un período, como mínimo, de 360 segundos (6 minutos), el direccionador eliminará la entrada correspondiente al vecino de la tabla de vecinos y, si el vecino es un nodo de servicio, de la tabla de direccionamientos.

H/W Addr

(Dir H/S) La dirección de LAN del nodo si el vecino está conectado a una LAN. Si se está ejecutando el protocolo Frame Relay, la H/W Addr será el identificador de conexión de enlace de datos (DLCI). Para las interfaces X.25, la H/W Addr es la dirección X.25 del vecino.

RIF

Campo de información del direccionamiento. Secuencia de números de puente y segmento, en hexadecimal, que indica una vía de acceso en la red entre dos estaciones. RIF es necesario para el direccionamiento de origen.

Implementación de RTP

Las entidades RTP emiten los paquetes siguientes:

- *Paquetes de solicitud RTP.* Solicitudes efectuadas a los nodos de servicio para obtener la topología de red actual. Durante la inicialización, una interfaz X.25 genera paquetes de solicitud de direccionamiento cada 90 segundos a cada destino X.25 de la interfaz X.25. Cuando la interfaz X.25 recibe un paquete de respuesta de direccionamiento, se envían tres actualizaciones completas de la base de datos de direccionamientos, separadas en períodos de 90 segundos, a los nodos de servicio que enviaron los paquetes de respuesta de direccionamiento. Cuando la interfaz X.25 haya recibido paquetes de respuesta de direccionamiento de todos los nodos de destino X.25, las solicitudes de direccionamiento ya no se enviarán a estas direcciones X.25.
- *Paquetes de actualización RTP.* Paquetes enviados por nodos cliente a los nodos de servicio para notificar a estos su existencia. Los nodos de servicio también envían estos paquetes para notificar su existencia a otros nodos y anunciar sus bases de datos de direccionamientos.
- *Paquetes de respuesta RTP.* Paquetes que envían los nodos de servicio como respuesta a los paquetes de solicitud RTP.
- *Paquetes de redireccionamiento RTP.* Informan a los nodos cuáles son las mejores vías de acceso existentes entre ellos para direccionar paquetes.

A menos que esté conectado mediante un circuito permanente, cada nodo cliente y de servicio difunde una actualización RTP cada 90 segundos. Esta actualización notifica a los vecinos la existencia del nodo, cuál es su tipo (nodo cliente o de servicio) y, en el caso de los nodos de servicio, anuncia sus bases de datos de direccionamientos. Cuando un direccionador recibe un paquete de actualización de un nodo de servicio, RTP extrae la dirección VINES IP y busca en la tabla de direccionamientos una entrada existente en dicho nodo de servicio. Si existe, RTP actualizará la entrada y restablecerá el temporizador de ésta. Si no existe una entrada, RTP creará una e inicializará el temporizador de ésta.

Internet Control Protocol (ICP)

ICP genera mensajes de información de la red sobre dos tipos de paquetes destinados al direccionador local:

- *Destination unreachable packet (Paquete cuyo destino no se puede alcanzar).* Indica que un paquete no ha podido llegar a su destino y que se ha devuelto a su origen. El direccionador emite entonces un mensaje ELS y desecha el paquete.
- *Delay metric packet. (Paquete de métrica retrasada).* Paquete de solicitud de un nodo de destino para saber la métrica de direccionamiento desde el nodo de servicio de destino hasta el nodo cliente de destino.

VINES Address Resolution Protocol (VINES ARP)

El protocolo VINES ARP asigna direcciones VINES IP únicas a los nodos cliente. VINES ARP incluye los tipos de paquete siguientes:

- *Paquete de solicitud de consulta.* Paquetes que los nodos cliente difunden al inicializar.
- *Paquete de respuesta de consulta.* Respuesta del nodo de servicios a un paquete de solicitud de consulta.
- *Paquete de solicitud de asignación.* Respuesta del nodo cliente a un paquete de respuesta de consulta.
- *Paquete de respuesta de asignación.* Incluye las direcciones de red y de subred que el nodo de servicio asignó al nodo cliente.

Para asignar una dirección VINES IP a un nodo cliente, VINES ARP implementa el algoritmo siguiente:

1. El nodo cliente difunde un paquete de solicitud de consulta.
2. Los nodos de servicio responden con un paquete de respuesta de consulta que contiene la dirección del MAC de destino del nodo cliente y una dirección VINES IP de difusión.
3. El nodo cliente emite un paquete de solicitud de asignación a un nodo de servicio que respondió con un paquete de respuesta de consulta.
4. El nodo de servicio responde con un paquete de respuesta de asignación que contiene las direcciones de subred y de red VINES.

Cada nodo cliente mantiene un temporizador que tiene una configuración por omisión de dos segundos. El temporizador se inicia cuando un nodo cliente transmite un paquete de solicitud de asignación o de solicitud de consulta. El nodo cliente detiene y restablece el temporizador cuando recibe un paquete de respuesta de consulta. Cuando un período de tiempo de espera supera los dos segundos, el nodo cliente se inicializa, difunde un paquete de solicitud de consulta y restablece el temporizador. La Tabla 101 resume los estados en los que entran los nodos de servicio y cliente durante la implementación de VINES ARP.

<i>Tabla 101 (Página 1 de 2). Estados VINES ARP de los nodos de servicio y cliente</i>	
Estados de los nodos cliente	
Inicialización	El nodo cliente se está inicializando.
Consulta	El nodo cliente está transmitiendo un paquete de solicitud de consulta.
Solicitud	El nodo cliente recibió un paquete de respuesta de consulta de un nodo de servicio y ahora está transmitiendo un paquete de solicitud de asignación al nodo de servicio que escuchó.
Asignado	El nodo cliente ha recibido un paquete de respuesta de asignación que contiene las direcciones de subred y de red VINES.
Estados del nodo de servicio	
Inicialización	El protocolo VINES ARP se está inicializando.
Escucha	El nodo de servicio está esperando paquetes de solicitud de consulta de los nodos cliente.
Servicio	El nodo de servicio ha recibido un paquete de solicitud de consulta y ha enviado un paquete de respuesta de consulta.

Tabla 101 (Página 2 de 2). Estados VINES ARP de los nodos de servicio y cliente

Asignación	El nodo de servicio emite un paquete de respuesta de asignación que contiene las direcciones de subred y red VINES.
------------	---

Procedimientos de configuración básicos

Los pasos para configurar inicialmente cada direccionador que envía y recibe paquetes VINES son los siguientes:

1. Asigne una dirección hexadecimal única de 32 bits a cada direccionador de la red VINES. Con el mandato **set network-address** *núm. hex*, entre una dirección de red que esté dentro del rango incluido entre 30900000 y 3097FFFF. La dirección de red de los servidores Banyan es el número de serie hexadecimal de 32 bits del nodo de servicio. Este número se lee automáticamente en la clave del servidor de nodos.
2. Habilite globalmente el protocolo VINES con el mandato **enable VINES**.
3. Habilite las tarjetas de interfaz que deban transmitir y recibir los paquetes de VINES con el mandato **enable interface** *núm.interfaz*.

Para que los cambios de configuración entren en vigor, debe reiniciar el direccionador. Entre **restart** o **reload** después del indicador OPCON (*) y responda **yes** a la solicitud siguiente:

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

Para ver la configuración, entre el mandato **list** después del indicador VINES config>.

Ejecución de Banyan VINES en el direccionador de puenteo

Los servidores de Banyan VINES deben tener esta opción de Banyan para comunicarse con otros servidores o direccionadores:

Server-to-server LAN (LAN de servidor a servidor).

Para comunicarse por WAN X.25, los servidores VINES conectados directamente a la WAN necesitan las dos opciones siguientes:

Server-to-server WAN (WAN de servidor a servidor)
Soporte de X.25 en el servidor (hardware y software).

Ejecución de Banyan VINES sobre enlaces de WAN

Cuando establezca un enlace PPP, Frame Relay o X.25 para usarlo con VINES, debe establecer la velocidad HDLC del enlace, incluso si establece el reloj en external (externo).

Si establece la velocidad de HDLC en cero, VINES presupondrá que la velocidad es de 56 kbps. No establezca la velocidad en un valor más rápido que la línea.

Configuración y supervisión de VINES

Este capítulo describe los mandatos de supervisión y configuración de VINES e incluye las secciones siguientes:

- “Acceso al entorno de supervisión de VINES” en la página 321
- “Mandatos de supervisión de VINES” en la página 321

Acceso al entorno de configuración de VINES

Para acceder al entorno de configuración de VINES, entre el mandato siguiente en el indicador Config>:

```
Config> protocol vin
VINES Protocol user configuration
VINES Config>
```

Mandatos de configuración de VINES

Esta sección resume y después explica los mandatos de configuración de VINES. Entre estos mandatos en el indicador VINES config>.

Tabla 102. Resumen de los mandatos de configuración de VINES

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte la sección “Cómo obtener ayuda” en la página xxix.
Add	Añade una conversión de dirección X.25.
Delete	Suprime una conversión de dirección X.25.
Disable	Inhabilita el protocolo VINES en todas las interfaces o en una única interfaz e inhabilita la suma de comprobación.
Enable	Habilita el protocolo VINES en todas las interfaces o en una única interfaz y habilita la suma de comprobación.
List	Muestra la configuración actual de VINES.
Set	Asigna las direcciones de red a direccionadores de la red VINES y establece el número máximo de nodos de servicio y de clientes vecinos físicos.
Exit	Le devuelve al nivel de mandatos anterior. Consulte la sección “Cómo salir de un entorno de nivel inferior” en la página xxix.

Add

Añade una conversión de dirección X.25.

Sintaxis:

```
add          interface ...
#           Especifica el número de interfaz.
```

Mandatos de configuración de VINES (Talk 6)

remote-X.25-addr

Puede incluir un máximo de 15 dígitos. Si ha configurado la conexión del circuito virtual como PVC, la *remote-X.25-addr* de VINES deberá coincidir con la dirección PVC configurada en el indicador de X.25. Si las direcciones no coinciden, el sistema pasará por omisión a un circuito virtual conmutado (SVC).

handle Nombre que puede configurar el usuario y que identifica de forma única a cada servidor remoto.

Ejemplo: `add interface 0 4508907898 test`

Delete

Suprime una conversión de dirección X.25.

Sintaxis:

`delete` `interface ...`

Especifica el número de interfaz.

remote-X.25-addr

Puede incluir un máximo de 15 dígitos. Si la interfaz especificada no se ha configurado con el mandato **add interface** de VINES, el terminal mostrará el mensaje That X.25 address has not been configured. (No se ha configurado esta dirección X.25).

Ejemplo: `delete interface 1 4799999999 compress`

Disable

Use el mandato **disable** para inhabilitar el protocolo VINES en todas las interfaces o en una única interfaz o para inhabilitar la suma de comprobación.

Sintaxis:

`disable` `checksumming ...`
 `interface ...`
 `vines`

checksumming *núm.interfaz*

Inhabilita la suma de comprobación en los paquetes que genera la interfaz específica, salvo los paquetes de difusión. En todas las interfaces, el valor por omisión es la inhabilitación de la suma de comprobación.

Ejemplo: `disable checksumming 0`

interface *núm.interfaz*

Inhabilita el protocolo VINES en la interfaz especificada.

Ejemplo: `disable interface 1`

vines Inhabilita el protocolo VINES en todas las interfaces.

Ejemplo: `disable vines`

Enable

Use el mandato **enable** para habilitar el protocolo VINES en todas las interfaces o en una única interfaz o para habilitar la suma de comprobación.

Sintaxis:

```
enable          checksumming ...
                  interface ...
                  vines
```

checksumming *núm.interfaz*

Habilita la suma de comprobación en los paquetes que genera la interfaz especificada.

Ejemplo: enable checksumming 0

interface *núm.interfaz*

Habilita el protocolo VINES en la interfaz especificada.

Ejemplo: enable interface 1

vines Habilita globalmente el protocolo VINES. Si recibe un mensaje de error después de entrar este mandato, póngase en contacto con el representante del servicio al cliente. Es posible que no tenga el software de VINES en la carga de software.

Ejemplo: enable vines

List

Use el mandato **list** para visualizar la configuración de VINES.

Sintaxis:

```
list
```

Ejemplo list

```
VINES: enabled/disabled
VINES network number (hex):
Maximum Number of Routing Table Entries:
Maximum Number of Neighbor Service Nodes:
Maximum Number of Neighbor Client Nodes:

List of interfaces configured for VINES:

intf 0      (checksumming enabled/disabled)
intf 1      (checksumming enabled/disabled)
intf 2      (checksumming enabled/disabled)
```

VINES X.25 Configuration

Interface	Remote X.25 Address	Remote Handle
0	4508907898	test

```
VINES config>
```

VINES Indica si VINES está globalmente habilitado o inhabilitado.

VINES network number (hex)

Dirección hexadecimal de 32 bits configurable para direccionadores de la red VINES.

Mandatos de configuración de VINES (Talk 6)

Maximum Number of Routing Table entries

Valor configurado que especifica el número máximo de entradas permitidas en la tabla de direccionamientos de VINES.

Maximum Number of Neighbor Service Nodes

Valor configurado que especifica el número máximo de nodos de servicio vecinos conectados al direccionador.

Maximum Number of Neighbor Client Nodes

Valor configurado que especifica el número máximo de nodos cliente conectados al direccionador.

List of interfaces configured for VINES

Muestra las interfaces que tienen VINES habilitado y si la suma de comprobación está habilitada o no.

VINES X.25 Configuration

Esta información representa los elementos siguientes:

Interface La interfaz configurada para X.25.

Remote X.25 Address

La dirección DTE del servidor remoto.

Remote Handle

Nombre que puede configurar el usuario y que identifica de forma única al servidor remoto.

Set

Use el mandato **set** para asignar direcciones de red a direccionadores de la red VINES y especificar el número máximo de nodos de servicio y cliente.

Sintaxis:

```
set          client-node-neighbors ...  
              network-address ...  
              routing-table-size ...  
              service-node-neighbors ...
```

client-node-neighbors número

Especifica el número máximo de nodos cliente de la red. **Client-node-neighbors** incluye todos los nodos de cada red que estén conectados directamente a través del direccionador. El rango está comprendido entre 1 y 65535 y el valor por omisión es 25.

Nota: Se recomienda que establezca este número en un valor que sea bastante más alto que el número de nodos de la red. Esto permitirá que la red siga funcionando sin tener que volver a configurar y reiniciar los direccionadores cuando se añaden nodos adicionales. El aumento de este número dependerá del tamaño de la red y del volumen de crecimiento anticipado. Por norma general, establezca **client-node-neighbors** en un valor que sea un 25 % superior al número real de estaciones cliente en las LAN que sean locales para el direccionador.

Ejemplo: `set client-node-neighbors 20`

network-address *número hexadecimal*

Asigna una dirección de red a cada direccionador de la red VINES. *número hexadecimal* es un valor hexadecimal de 32 bits incluido entre 30900000 y 3097FFFF.

Ejemplo: set network-address 30922222

routing-table-size *número*

Especifica el número máximo de direccionadores y nodos de servicio en la red VINES. El rango está comprendido entre 1 y 65535 y el valor por omisión es 300.

Nota: Asegúrese de que el número que especifique sea lo suficientemente grande como para acomodar servidores VINES y 2210 adicionales a medida que crece la red.

Ejemplo: set routing-table-size 250

service-node-neighbors *número*

Especifica el número máximo de nodos de servicio vecinos físicos. El número incluye los servidores VINES y 2210 que son el primer punto de contacto después de atravesar una WAN. El rango está comprendido entre 1 y 65535 y el valor por omisión es 50.

Ejemplo: set service-node-neighbors 100

Acceso al entorno de supervisión de VINES

Para acceder al entorno de supervisión de VINES,

```
* t 5
```

A continuación, entre el mandato siguiente en el indicador +:

```
+ protocol vin
VINES>
```

Mandatos de supervisión de VINES

Esta sección describe los mandatos de supervisión de VINES. Entre estos mandatos en el indicador VINES>.

Tabla 103 (Página 1 de 2). Resumen de los mandatos de supervisión de VINES

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte la sección "Cómo obtener ayuda" en la página xxix.
Counters	Muestra los errores de direccionamiento y el número de veces que la cola de entrada de VINES estaba llena cuando se recibieron paquetes de la interfaz especificada.
Dump	Muestra el contenido actual de las tablas vecinas y de direccionamientos de VINES.
Route	Muestra una entrada de la tabla de direccionamientos de VINES.

Tabla 103 (Página 2 de 2). Resumen de los mandatos de supervisión de VINES

Mandato	Función
Exit	Le devuelve al nivel de mandatos anterior. Consulte la sección "Cómo salir de un entorno de nivel inferior" en la página xxix.

Counters

Use el mandato **counters** para visualizar los errores de direccionamiento y el número de veces que la cola de entrada de VINES estaba llena cuando se recibieron paquetes de la interfaz especificada.

Sintaxis:

counters

Ejemplo: counters

```

Routing Errors
Count      Type
-----
  2        Net Unreachable
  3        Hop Count Expired
  3        Routing Update from Orphan Client
  0        Routing Redirect Received
  0        Routing Response Received

VINES Input Packet Overflows
Net        Count
---
Eth/0      5
Eth/1      1
    
```

Net Unreachable

(Imposible llegar a la red) Número de veces que el direccionador recibió un paquete destinado a un nodo que no estaba en la tabla de direccionamientos.

Hop Count Expired

(Cuenta de saltos agotada) Número de veces que el direccionador descartó un paquete porque la cuenta de saltos se había agotado.

Routing Update from Orphan Client

(Actualización de direccionamiento de un cliente huérfano) Número de veces que el direccionador recibió un paquete de actualización de un nodo cliente cuyo nodo de servicio no existía. Puede producirse una actualización de direccionamiento de un cliente huérfano cuando el direccionador arranca y oye primero al nodo cliente en vez de oír al nodo de servicio o bien, cuando un nodo de servicio del cliente está desactivado y se ha eliminado una entrada de la base de datos de direccionamientos.

Routing Redirect Received

(Redireccionamiento de ruta recibido) Número de veces que el direccionador recibió paquetes redireccionados de nodos de servicio.

Routing Response Received

(Respuesta de direccionamiento recibida) Número de veces que se generaron paquetes de respuesta como consecuencia de paquetes de solicitud iniciados por el direccionador.

VINES input packet overflows

(Desbordamiento de paquetes de entrada VINES) Número de veces que la cola de entrada del reenviador de VINES estaba llena cuando se recibieron paquetes de la interfaz especificada. Los paquetes se descartaron después.

Dump

Use el mandato **dump** para mostrar el contenido de las tablas vecinas y de direccionamientos de VINES.

Sintaxis:

```
dump          neighbor-tables
                routing-tables
```

neighbor-tables

Muestra información sobre cada nodo cliente y de servicio de vecinos conectados al direccionador.

Ejemplo: **dump neighbor-tables**

Nbr Address	Intf	Metric	Age(secs)	H/W Addr	RIF
30622222:0001	TKR/0	4	30	0000C00	95012
0035CC10:8000	Eth/0	2	120	0000C00	78221

2 Total Neighbors

Nbr Address

(Dirección vcn) La dirección del nodo vecino. En el ejemplo anterior, la dirección 30622222:0001 es un nodo de servicio y la dirección 0035CC10:8000 es un nodo cliente.

Intf (Intf.) El soporte al que está conectado el nodo vecino.

Metric (Métrica) Costo estimado, en 200 milisegundos, de direccionar el paquete VINES al nodo vecino.

Age (secs)

(Edad - segs) Edad actual de la entrada en segundos. Si un direccionador no recibe una actualización de direccionamiento de un vecino en un período, como mínimo, de 360 segundos (6 minutos), el direccionador eliminará la entrada correspondiente al vecino de la tabla de vecinos y, si el vecino es un nodo de servicio, de la tabla de direccionamientos.

H/W Addr

(Dir H/S) La dirección de LAN del nodo si el vecino está conectado a una LAN. Si se está ejecutando el protocolo Frame Relay, la H/W Addr será el identificador de conexión de enlace de datos (DLCI). Para las interfaces X.25, la H/W Addr es la dirección X.25 del vecino.

RIF Campo de información del direccionamiento. Secuencia de números de puente y segmento, en hexadecimal, que indica una vía de acceso en la red entre dos estaciones. RIF es necesario para el direccionamiento de origen.

routing-tables

Muestra información sobre cada nodo de servicio que conoce el direccionador.

Ejemplo: dump routing-table

Net Address	Next Hop	Nbr Addr	Nbr Intf	Metric	Age (secs)
S 30622222	30622222:0001		Eth/0	20	30
H 0027AA21	0027AA21:0001		Eth/1	2	120
P 0034CC11	0034CC11:0001		X.25/0	45	0

3 Total Routes

S ==> Entry is suspended, H ==> Entry is Holdown, P ==> Entry is permanent

Net Address

(Dirección de la red) La dirección de la red es un número exclusivo hexadecimal de 32 bits, que se puede configurar con un valor del rango incluido entre 30900000 y 3097FFFF. Banyan ha asignado este rango de números a IBM. Es muy importante que no se asigne la misma dirección de red a dos direccionadores de una misma red. La dirección de red de un nodo de servicio Banyan es un número de serie hexadecimal de 32 bits del nodo de servicio. Si delante del campo de dirección de la red se encuentra una S, una H o una P, los significados serán los siguientes:

- S:** El nodo de servicio está suspendido y se anuncia que está desactivado durante 90 segundos. Después de este tiempo, el direccionador elimina la entrada correspondiente a este nodo de la tabla de direccionamientos.
- H:** El nodo de servicio está retenido y se anuncia que está desactivado durante 2 minutos. Después de este tiempo, el direccionador anunciará que el nodo de servicio está operativo. Si un nodo de servicio está suspendido y recibe un paquete RTP, el nodo de servicio entrará en estado de retención.
- P:** Después de la inicialización, la interfaz X.25 entra en estado permanente durante 4 minutos y medio. Después de este tiempo, el vecino entrará en dicho estado y su edad permanecerá en 0 mientras se encuentre así. Si la interfaz X.25 se desactiva, se eliminará la entrada de la tabla de direccionamientos.

Next Hop Nbr Addr

(Dirección vecino salto siguiente) Dirección del nodo de servicio vecino que es el salto siguiente de la vía de acceso de menos costo a la red.

Nbr Intf (Intf. vecino) El soporte al que el nodo de servicio vecino del salto siguiente está conectado.

Metric (Métrica) Costo estimado, en 200 milisegundos, de direccionar el paquete VINES al nodo de servicio de destino.

Age (secs)

(Edad - secs) Edad actual de la entrada en segundos. Si un direccionador no recibe una actualización de direccionamiento de un nodo de servicio que está en la tabla de direccionamientos cada 360 segundos (6 minutos) como mínimo, el direccionador eliminará la entrada correspondiente al nodo de servicio de la tabla de direccionamientos.

Route

Use el mandato **route** para ver una entrada de la tabla de direccionamientos.

Sintaxis:

route given address

given address

La dirección de red del nodo de servicio.

Ejemplo: route 30622222

Net Address	Next Hop	Nbr Addr	Nbr Intf	Metric	Age (secs)
30622222	30622222:0001		Eth/0	2	30

Mandatos de supervisión de VINES (Talk 5)

Uso de DNA IV

Este capítulo describe la implementación de Digital Network Architecture Phase IV (DNA IV) que efectúa IBM e incluye las secciones siguientes:

- “Visión general de DNA IV”
- “Implementación de DNA IV efectuada por IBM” en la página 331
- “Configuración de DNA IV” en la página 340
- “Mandatos de configuración y supervisión de DNA IV” en la página 345

Visión general de DNA IV

DNA IV es un conjunto de componentes de software que transfieren información entre redes conectadas mediante un soporte físico. Al transferir información, el software DNA IV facilita la comunicación entre los dispositivos de red como, por ejemplo, sistemas personales, servidores de archivos e impresoras.

El protocolo DNA IV es el protocolo subyacente de los productos de software DECnet de Digital Equipment Corporation así como de los productos compatibles con DNA. Este protocolo incluye:

- Software de direccionamiento para redes de protocolo DNA IV.
- NCP, una implementación de DNA IV Network Control Program (programa de control de red DNA IV). Para obtener más información, consulte la documentación de DECnet-VAX adecuada, publicada por Digital Equipment Corporation.
- Soporte del Maintenance Operations Protocol (MOP) de DNA IV.

DNA IV lleva a cabo dos funciones principales:

- Mantiene una base de datos completa de direccionamientos en todos los nodos de su área. (Si el direccionador funciona como direccionador de nivel 2, mantiene también la base de datos para todas las áreas).
- Direcciona paquetes de datos DECnet de entrada a los destinos adecuados basándose en su propia base de datos de direccionamientos. Ignora los paquetes destinados al direccionador que no sean paquetes hello o de direccionamiento.

DNA IV da soporte a:

- Varias áreas en una red Ethernet o red en anillo .
- Operaciones de MOP básicas. DNA IV responde a un mensaje de ID de solicitud de MOP con un mensaje de ID de sistema de MOP. DNA IV también envía un mensaje de ID de sistema de MOP cuando se activa un circuito. Puede supervisar mensajes de MOP usando el módulo de configuración Ethernet bajo DECnet-VAX NCP. El NCP del direccionador no incluye un módulo de configuración de Ethernet.
- Protocolo LAT. El protocolo LAT no forma parte de la familia de protocolos DNA IV. Se trata de un protocolo destinado únicamente a Ethernet que sólo se ocupa de comunicaciones de corta distancia (tiempo de ida y vuelta limitado). (El protocolo CTERM proporciona soporte de terminales de área amplia usando protocolos DNA IV en los direccionadores). El mandato **set host** en DECnet-VAX proporciona el protocolo CTERM).

Debe prestarse una atención especial a las restricciones siguientes de DNA IV:

- DNA IV no da soporte a los protocolos NSP, Session o NICE.
- DNA IV no da soporte al protocolo de línea DDCMP en las líneas síncronas directamente conectadas.
- DNA IV no proporciona ninguna función de compatibilidad de Phase III ya que no da soporte a los protocolos de enlace de datos DDDCMP usados por todos los nodos Phase III.
- NCP (la implementación efectuada por el direccionador del DECnet Network Control Program) implementa un subconjunto de funciones y mandatos de NCP originales.

Terminología y conceptos de DNA IV

Esta sección contiene una breve descripción de la terminología DNA IV.

Direccionamiento

Cada nodo tiene una dirección de nodo de 16 bits, la cual es la misma para todas las interfaces de dicho nodo. Una dirección está formada por 2 campos: 6 bits de número de área y 10 bits de número de nodo. Las direcciones se imprimen en números decimales con un punto que separa el área; por ejemplo, 1.7 es el nodo 7 del área 1. Si no se indica ningún área se presupone el área 1. Cualquier dirección que esté en el rango incluido entre 1.1 y 63.1023 es legal. Ambos nodos y áreas deben empezar a numerarse a partir del 1 con poca holgura, si la hay. Esto se produce porque el número de nodo máximo y los números de área máximos son opciones de configuración y controlan el tamaño de varias estructuras de datos de direccionamiento.

No hay correlación directa entre las direcciones y el cableado físico. Las rutas se calculan en los nodos y no en los cables.

Direccionamiento de enlaces de datos Ethernet

Cada interfaz de Ethernet se establece en la misma dirección física de 48 bits, la cual es la concatenación de un prefijo de 32 bits (AA-00-04-00) y la dirección de nodo DNA IV de 16 bits. La dirección de nodo se conmuta por bytes (para convertir de PDP11 al orden de bytes de Ethernet). Por consiguiente, el nodo de DNA IV 1.1 tiene la dirección de Ethernet AA-00-04-00-01-04.

La difusión múltiple (no la difusión general) también se usa en el direccionamiento. Las tres direcciones de difusión múltiple usadas por DNA IV son AB-00-00-02-00-00, AB-00-00-03-00-00 y AB-00-00-04-00-00.

Direccionamiento de enlace de datos de red en anillo 802.5

La implementación de DNA sobre IEEE 802.5 Token Ring respeta la *DECnet Digital Networking Architecture (Phase IV) Token-Ring Data Link and Node Product Functional Specification*, Versión 1.0.0, que incluye soporte para direcciones de MAC arbitrarias (AMA).

Existen dos tipos de direccionamiento MAC, el direccionamiento DNA IV convencional, que es la concatenación de un prefijo de 32 bits (AA-00-04-00) y la dirección de nodo/área de DNA IV de 16 bits o AMA que permite al protocolo DNA ejecutarse en nodos IEEE 802.5 sin que este protocolo tenga que cambiar las direcciones de MAC. Esto es necesario si sigue algunas convenciones de protocolo

IBM. Puede seleccionar el tipo de direccionamiento que está usando a través del proceso de configuración de DNA (NCP>).

Otro tipo de representación del direccionamiento es el orden de bits nativo. Cuando se envía en la capa física, este tipo de dirección está agrupada por bytes. Por ejemplo, el prefijo de 32 bits canónico que se muestra arriba (utilizando guiones) se expresa como 55:00:20:00 en orden de bits nativos con el signo de dos puntos separando cada byte.

Nota: Cuando se configura DNA IV para ejecutarse sobre ATM LAN Emulation, debe usarse el AMA.

Direccionamiento de enlace de datos X.25

El direccionador da soporte a DECnet Phase IV sobre X.25 y puede funcionar con direccionadores que ejecuten la implementación de Digital de DECnet Phase IV sobre X.25.

La dirección DTE remota y local se establece con el mandato **set/define circuit** cuando establece un circuito DECnet. En el parámetro *call-userdata* se especifica la dirección DTE local en octetos hexadecimales (caracteres). En el parámetro *DTE-address*, se especifica la dirección remota en octetos hexadecimales. Tanto la dirección DTE remota como local pueden tener un máximo de 14 octetos hexadecimales de longitud con dos caracteres ASCII que representen un octeto hexadecimal.

Direccionamiento

DNA IV maneja tanto el reenvío de paquetes de datos DNA IV como el direccionamiento automático con otros nodos DNA IV. El direccionador ejecuta las funciones de DNA IV siguientes:

- Anuncia su presencia enviando mensajes hello a todas las redes que tienen habilitado DNA IV.
- Mantiene una lista de nodos DNA IV adyacentes a partir de los paquetes hello que recibe de otros nodos DNA IV.
- Intercambia información de direccionamiento con otros direccionadores.
- Reenvía paquetes entre nodos.

Todos los nodos de direccionamiento y finales difunden periódicamente mensajes hello a la dirección de difusión múltiple de todos los direccionadores. Esto permite que cada direccionador localice otros nodos de su área.

En cada red de difusión (por ejemplo, Ethernet, red en anillo), un direccionador se declara a sí mismo como direccionador designado para ese cable. Dicho direccionador difunde su presencia para que los nodos finales sepan cómo utilizarlo como pasarela por omisión. Cualquier nodo final que envíe un paquete a un nodo que no esté en ese cable lo enviará automáticamente al direccionador designado para que lo reenvíe.

En una DNA multiárea, asigne prioridades a direccionadores de tal manera que el direccionador designado sea un direccionador de nivel 2 o bien que probablemente sea el salto siguiente con más posibilidades para los destinos usados con más frecuencia. Esto reduce la posibilidad de que el tráfico de los nodos finales tenga que añadir un salto adicional.

Las decisiones de direccionamiento se basan en un algoritmo de menos costo. Cada enlace (por ejemplo, de punto a punto, red de difusión, salto) tiene un costo. Cada direccionador difunde (únicamente a otros direccionadores) su costo y el número de saltos para llegar a cada nodo de su área. Así, cada direccionador busca la vía de acceso más barata, en relación a una cuenta de saltos máxima.

Tablas de direccionamiento

Un direccionador reenvía al nodo adecuado, basándose en su tabla de direccionamientos, el paquete de datos DNA IV que recibe. A fin de mantener dicha tabla, un direccionador escucha las actualizaciones de nivel 1 y las envía a cada nodo de su área. Si el tipo del direccionador se establece en AREA, también intercambia actualizaciones de direccionamiento de nivel 2.

Cada direccionador mantiene una tabla de direccionamientos con una entrada por cada nodo (hasta la dirección máxima) y cada salto siguiente posible (todos los circuitos y hasta el máximo de direccionadores de difusión). Cada entrada de esta tabla contiene el costo y el salto para alcanzar un nodo a través de un circuito o el nodo del salto siguiente. Cada segundo la tabla de direccionamientos envía un temporizador de direccionamientos de difusión.

Direccionadores de áreas

Si se configura el direccionador como direccionador de áreas, éste mantendrá una base de datos similar para todas las áreas hasta el área máxima y podrá intercambiar información de direccionamiento de áreas con otros direccionadores de áreas. Las áreas se manejan casi de la misma manera que los nodos, salvo que los mensajes dan costos a las áreas, pero no a los nodos.

El concepto de áreas da como resultado dos tipos de nodos de direccionamientos:

- Un direccionador de nivel 1 sólo conoce un área, por lo que mantiene un seguimiento de los nodos del área. Además, no tiene en cuenta las adyacencias a través de las áreas.
- Un direccionador de nivel 2 mantiene una base de datos de direccionamientos de áreas y puede tener adyacencias a través de áreas. Los direccionadores de nivel 2 anuncian rutas al resto de las áreas, por lo que los direccionadores de nivel 1 envían todo el tráfico de áreas externas a los direccionadores de nivel 2.

Los nodos finales pasan simplemente paquetes a un direccionador.

Un direccionador de nivel 2 que puede alcanzar otras áreas anuncia una ruta a un nodo 0 dentro de su área. Cuando los direccionadores de nivel 1 necesitan enviar un paquete a otra área, lo direccionan hacia el nodo 0 más cercano. Esto no significa que sea la mejor ruta a dicha área. Desde ahí, el algoritmo de direccionamiento de nivel 2 envía el paquete a su área de destino.

Configuración de los parámetros de direccionamiento

En cada sistema puede establecer los parámetros de direccionamiento siguientes:

- Número máximo de nodos en el área
- Número máximo de direccionadores adyacentes a este direccionador
- Número máximo de redes en cualquier nodo determinado

- Número máximo de nodos finales que están a un salto de este nodo final
- Costo de un salto en cada red a la que está conectado este nodo
- Valores de varios temporizadores implicados en enviar mensajes hello y que los esperan de otros nodos

Implementación de DNA IV efectuada por IMB

El principal programa de interfaz de usuario para la implementación de direccionador de DNA IV se llama NCP. El NCP del direccionador es un subconjunto limitado de mandatos de DECnet Network Control Program (NCP). El NCP del direccionador habilita al usuario para visualizar y modificar los diversos argumentos de funcionamiento de DNA IV y leer diversos contadores específicos de DNA.

Algunas de las características del NCP del direccionador incluyen:

- NCP implementa entidades nuevas: control de acceso de módulos y filtro de direccionamiento de módulos.
- NCP no tiene mandato **set executor buffer size** ya que el direccionador no origina tráfico DECnet. El direccionador puede reenviar el paquete más grande que cualquier implementador DECnet puede generar. Cumple las restricciones de tamaño del almacenamiento intermedio en todos los nodos adyacentes.
- NCP permite un calificador **all** en los submandatos **node**, **area** y **circuit**.

El NCP del direccionador es similar al NCP de DECnet-VAX, con las diferencias siguientes:

- El NCP del direccionador no incluye el mandato **set node name** y, por consiguiente, no puede asignar nombres a nodos o visualizar nombres de nodos con direcciones.
- El NCP del direccionador no incluye los mandatos **clear** o **purge** ni los mandatos **set** tienen un argumento **all**. La base de datos permanente siempre se copia en la base de datos volátil cuando se inicia, reinicia o arranca el direccionador.
- Un mandato del NCP del direccionador puede tener únicamente un argumento.
- NCP no tiene el concepto de líneas. Para ver los datos que un mandato **show line** del NCP DECnet-VAX muestra, use los mandatos **interface** y **network** de GWCON.
- El NCP del direccionador no da soporte a mandatos entre redes:
 - El NCP del direccionador no incluye el mandato **tell**, el cual solicita mandatos de NCP en otros nodos.
 - Asimismo, el NCP del direccionador no da soporte a solicitudes de protocolo de soporte de otros direccionadores DNA para ejecutar mandatos del NCP en el direccionador en su nombre.

Importante

Antes de configurar DNA IV, es necesario que sea consciente de las características de seguridad opcionales tratadas en:

- “Gestión de tráfico utilizando el control de acceso” en la página 332
 - Proporciona seguridad limitando el acceso en los direccionadores de la red.
- “Gestión del tráfico con filtros de direccionamiento de áreas” en la página 335
 - Limita el acceso a grupos de áreas de otras áreas
 - Permite la fusión de dos espacios de direcciones de DECnet

Si ya está familiarizado con estos temas, salte las dos secciones mencionadas y empiece a leer en “Configuración de DNA IV” en la página 340.

Gestión de tráfico utilizando el control de acceso

El control de acceso protege a un grupo de nodos de otros nodos de la red. Los direccionadores hacen que todos los nodos de una red sean accesibles entre sí. Por lo general, las principales formas de seguridad son las contraseñas y el uso conservador del acceso proxy de DNA IV en el nivel del sistema principal.

No obstante, debido a diferencias en el nivel de seguridad de las máquinas, es posible que deba proveer seguridad adicional limitando el acceso dentro de los direccionadores de la red. El reenviador de DNA le habilita para ello mediante los controles de acceso.

Por lo general, no se recomienda los controles de acceso debido a:

- Los controles de acceso influyen en el rendimiento de un direccionador ya que se prueba cada paquete. Cuanto más complicada sea la configuración del control de acceso, mayor influencia tendrá en el rendimiento.
- Los controles de acceso son difíciles de configurar y los errores de configuración difíciles de diagnosticar.
- Los controles de acceso no pueden ocultar un nodo a los protocolos de direccionamiento. El nodo sigue estando visible para todos los direccionadores de su área.

Nota: Los controles de acceso no garantizan la seguridad; sólo dificultan las intrusiones. Los protocolos de direccionamiento DNA IV usados en Ethernet y otros soportes de difusión no tienen características de seguridad incorporadas.

El control de acceso evita el reenvío de paquetes de datos de DNA IV (formato largo) basándose en la dirección de origen, dirección de destino e interfaz. Este control no influye en los paquetes de direccionamiento, ya que usan un formato de paquete diferente. Esto da mayor seguridad a la configuración del control de acceso, ya que no puede interrumpir el protocolo de direccionamiento.

Para implementar el control de acceso, las direcciones se enmascaran y comparan. Es decir, se pone una máscara a la dirección en cuestión con 1 en las posiciones de los bits que deben probarse y 0 en el área libre. A continuación, la

dirección se compara con un valor fijado. Por ejemplo, puede usar una máscara de 63.1023 (todo 1) y compararla con un resultado de 6.23, lo cual es cierto únicamente para el nodo 6.23. Puede usar una máscara de 63.0 y un resultado de 9.0, lo cual es cierto para cualquier nodo del área 9.

Esta máscara y los valores de comparación vienen en pares para la dirección de origen y la destino. A continuación, se forman en listas para una interfaz. Cada interfaz tiene una lista de control de acceso, la cual aplica a los paquetes que recibe. La lista puede ser incluyente o excluyente. Una lista incluyente es un conjunto de pares de direcciones que designan un corredor para el flujo de tráfico. Una lista excluyente es un conjunto de pares de direcciones que no permiten el flujo de tráfico.

En una lista incluyente, las direcciones de origen y de destino se prueban usando la máscara y los valores de comparación. Si el origen y el destino de una entrada coinciden, se reenviará el paquete. En una lista excluyente, las direcciones de origen y de destino se prueban usando la máscara y los valores de comparación. Si el origen y el destino de una entrada coinciden, se eliminará el paquete. La elección entre incluyente y excluyente debe realizarse basándose en qué lista será más corta. No obstante, el control de acceso excluyente es, por lo general, más fácil de configurar.

Cuando se eliminan paquetes debido a controles de acceso, se establece el bit Return to Sender Request (Solicitud de retorno a transmisor - RQR) en la cabecera del paquete de datos de formato largo y se devuelve el paquete. A continuación, la solicitud de conexión falla inmediatamente ya que normalmente se envían los paquetes NSP Connect Initiate (iniciación de conexión NSP) con el bit RQR establecido.

Configuración del control de acceso

El control de acceso limita el acceso a un sistema principal o un grupo de sistemas principales determinados. Debe asignar el control de acceso a todos los direccionadores a dicho sistema principal y no sólo al direccionador preferido. De lo contrario, el control de acceso funcionará cuando la ruta primaria esté activada pero fallará cuando se use la secundaria.

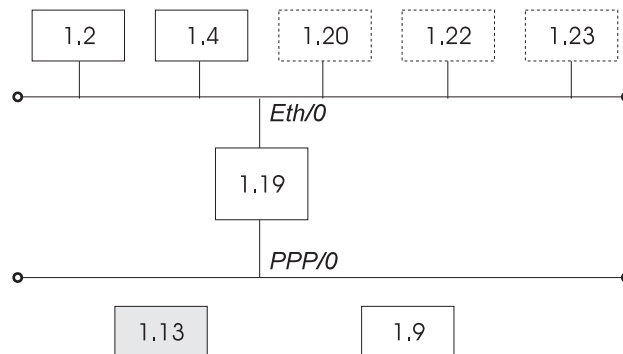
En el mapa de la red, trace una línea para aislar la región fiable del resto de la red. La línea ideal debería cruzar el conjunto de adyacencias menor posible para que se ejecute el menor número posible de interfaces con control de acceso. En el caso de las redes de difusión (Ethernet y red en anillo), trace la línea a través del cable de interconexión al nodo para identificar la interfaz con el filtro. Por cada interfaz que la línea de control de acceso cruce, use NCP para definir la misma lista de control de acceso.

Nota: Dado que todas las aplicaciones DECnet usan el protocolo NSP, el cual necesita una conectividad bidireccional, no es necesario definir el control de acceso en ambas direcciones.

Control de acceso incluyente

En la Figura 15 en la página 334, el nodo 1.13 desea comunicarse únicamente con los nodos 1.2 y 1.4. El control de acceso le permite dar fiabilidad a algunos nodos entre todos los nodos que tienen conexión de direccionadores. Por consiguiente, en la Figura 15 en la página 334 puede proteger el nodo 1.13 de todos los nodos salvo del nodo 1.9 ya que ambos nodos comparten la misma red física.

Para configurar el control de acceso deseado para este ejemplo, cree un filtro incluyente en la interfaz Eth/0 del direccionador 1.19, tal como se muestra en la parte inferior de la Figura 15 en la página 334



Información del filtro incluyente

Resultado de origen	Máscara de origen	Resultado de destino	Máscara de destino
1.2	63.1023	1.13	63.1023
1.4	63.1023	1.13	63.1023
0.0	0.0	1.9	63.1023

Figura 15. Ejemplo de un control de acceso incluyente

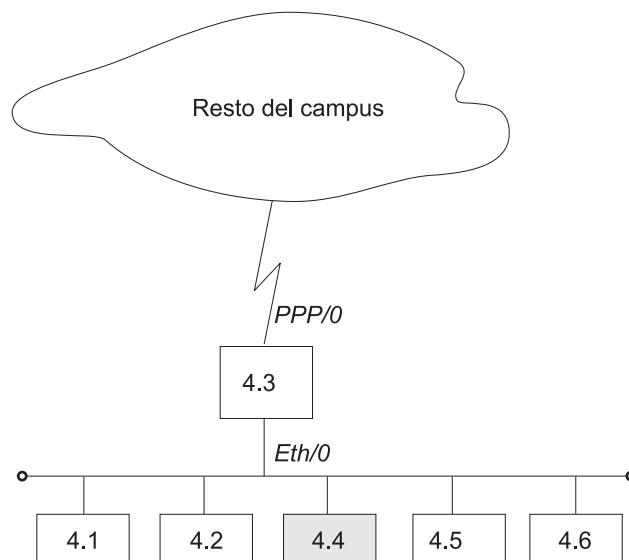
La primera y la segunda entradas de la información del filtro incluyente que aparecen en la Figura 15 permiten a los nodos 1.2 y 1.4 enviar paquetes al nodo 1.13. La tercera entrada permite que todos los nodos hagan envíos al nodo 1.9 (no está intentando dar fiabilidad al nodo 1.9).

Para configurar el ejemplo indicado para el direccionador 1.19, entre los parámetros y mandatos de NCP siguientes:

```
NCP> def mod access-cont circ eth/0 type inclusive
NCP> def mod access-cont circ eth/0 filter 1.2 63.1023 1.13 63.1023
NCP> def mod access-cont circ eth/0 filter 1.4 63.1023 1.13 63.1023
NCP> def mod access-cont circ eth/0 filter 0.0 0.0 1.9 63.1023
NCP> def mod access-cont circ eth/0 state on
```

Control de acceso excluyente

La Figura 16 en la página 335 muestra cómo el control de acceso excluyente aísla el nodo 4.4 del resto del campus.



Información del filtro excluyente

Resultado de origen	Máscara de origen	Resultado de destino	Máscara de destino
0.0	0.0	4.4	63.1023

Figura 16. Ejemplo de control de acceso excluyente

Configure el control de acceso deseado para este ejemplo creando un filtro excluyente en la interfaz PPP/0 del direccionador 4.3, tal como se muestra en la Figura 16. Para configurar el ejemplo indicado para el direccionador 4.3 en la Figura 16, entre los parámetros y mandatos de NCP siguientes:

```
NCP> def mod access-cont circ ppp/0 type exclusive
NCP> def mod access-cont circ ppp/0 filter 0.0 0.0 4.4 63.1023
NCP> def mod access-cont circ ppp/0 state on
```

Gestión del tráfico con filtros de direccionamiento de áreas

Los filtros de direccionamiento de áreas permiten efectuar configuraciones especiales de la red DNA. Dado que se trata de un tema avanzado, muy pocas redes DNA IV necesitan filtros de direccionamiento. En DNA IV existen dos aplicaciones primarias para el filtro de áreas:

- Seguridad; se limita el acceso a algunos grupos de áreas de otras áreas.
- Se permite la fusión de dos espacios de direcciones de DECnet.

Nota: La configuración de los filtros de direccionamiento de áreas es muy delicada y está plagada de dificultades. Es muy fácil romper totalmente el direccionamiento de áreas. Si no comprende cómo funciona el direccionamiento de DECnet, especialmente en el nivel de las áreas, no intente usar filtros de direccionamiento. Puede encontrar documentación sobre el protocolo de direccionamiento DECnet en *DECnet Digital Network Architecture Phase-IV Routing Layer Functional*

Description, número de pedido AAX435ATK, Diciembre de 1983, Digital Equipment Corporation, Maynard, Massachusetts.

Los filtros de direccionamiento de áreas le permiten configurar un direccionador para controlar la información sobre áreas DECnet que se envían o aceptan en los mensajes de direccionamiento de nivel 2. Por cada interfaz, puede configurar varios filtros separados de entrada o salida. Cada filtro especifica qué información de direccionamiento de áreas se pasará o aceptará.

Cuando una red envía una actualización de direccionamiento de nivel 2 y hay un filtro de direccionamiento, la entrada (RTGINFO) de cualquier área que no esté en el filtro tendrá el costo de 1023 y una cuenta de saltos de 63. Cada área del filtro tiene el costo y los saltos correctos en la entrada.

Cuando la red recibe un mensaje de direccionamiento de nivel 2 y hay un filtro de direccionamiento, las entradas de un área que no esté en el filtro se tratarán como si el costo fuese 1023 y la cuenta de saltos 63 (inalcanzable). Cualquier entrada de direccionamiento del paquete que esté en el filtro se procesará normalmente.

Los filtros de direccionamiento únicamente influyen en el proceso de los mensajes de direccionamiento de nivel 2. No hay filtros para los mensajes de direccionamiento de nivel 1. Los filtros de direccionamiento no influyen en el proceso de hello del direccionador y no evitan que los direccionadores de áreas desarrollen adyacencias. Sí, influyen, por el contrario, en la base de datos de direccionamientos de áreas. Si los filtros evitan que un direccionador de áreas obtenga conocimientos de otra área, evitarán que el direccionador se conecte y, por consiguiente, éste no podrá anunciarse como direccionador de áreas.

Seguridad mediante filtro de áreas

Al igual que los controles de acceso, los filtros de direccionamiento proporcionan seguridad. No obstante, los filtros de direccionamiento tienen algunos inconvenientes si se comparan con los controles de acceso:

- El filtro de áreas es menos flexible que los accesos de control ya que requieren que la asignación de áreas corresponda con la arquitectura de seguridad deseada.
- El filtro de áreas es más difícil de comprender y configurar.
- El nivel de seguridad es inferior ya que, de todas formas, un sistema principal que no tenga en cuenta la información de direccionamiento puede enviar los paquetes al direccionador correcto.

No obstante, el filtro de áreas es más eficaz ya que no es necesario comprobar cada paquete. En el ejemplo siguiente, el filtro de áreas se produce en un área que contiene estaciones de trabajo que forman parte de una red grande que contiene máquinas con información confidencial. Puede darse el caso de que las máquinas confidenciales deban ponerse en contacto con una máquina de fuera del área para obtener información.

En la Figura 17 en la página 337, el área 13 contiene estaciones de trabajo que deben poder llegar al área 1. El nodo 13.1 es el direccionador y los otros nodos son las estaciones de trabajo. El nodo 13.1 tiene un filtro que sólo acepta rutas al área 7. Por consiguiente, si el nodo 13.1 recibe un paquete de cualquier nodo del área 13 que no esté destinado al área 7, no podrá reenviar el paquete y enviará al nodo de envío un mensaje de error.

Para configurar el direccionador 13.1 de la Figura 17 en la página 337, entre los parámetros y mandatos siguientes de NCP:

```
NCP> def mod routing-filter circ eth/1 incoming area 7
NCP> def mod routing-filter circ eth/1 incoming state on
```

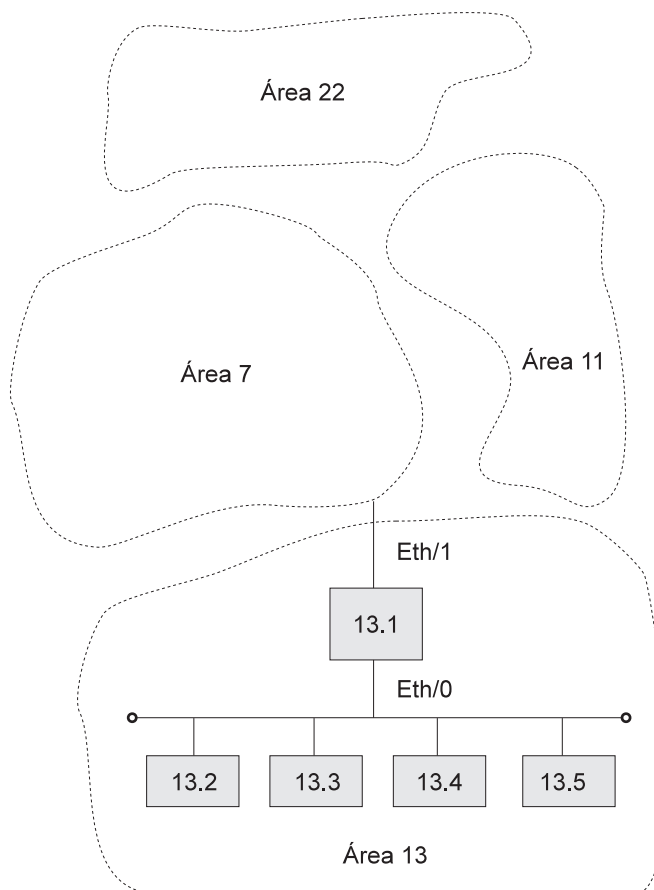


Figura 17. Ejemplo de filtro de direccionamiento de áreas para seguridad

Fusión de dominios DECnet

DECnet tiene un espacio de dirección de nodo de 16 bits con una jerarquía fijada de 6 bits de área y 10 bits de nodo. En comparación, IP tiene un espacio de dirección de nodo de 32 bits con una jerarquía multinivel flexible. Ahora, varias redes establecidas han crecido hasta el punto de usar las 63 áreas. El problema que se plantea es que, a medida que se conectan diferentes recursos entre sí, éstos desean conectar sus redes DECnet pero no es posible debido a conflictos de número de área.

La única solución consiste en volver a diseñar la arquitectura de DECnet. (DECnet Phase V trata esta cuestión). No obstante, al usar filtros de direccionamiento de áreas, es posible permitir un cierto solapamiento entre dos dominios DECnet.

Dominio no es un término estándar de DECnet, lo utilizamos aquí como nombre de una red de área amplia DECnet, presumiblemente una red con varias áreas. El objetivo es fusionar dos de estos dominios para que haya un área común que pueda llegar a partes de ambos dominios. No obstante, en la unión de dos dominios hay más de 63 áreas. Dado que el filtro de áreas no es fácil de administrar y

es restrictivo, no lo use si tiene suficientes números de área disponibles para la unión de los dominios.

Para configurar la solapación de dos dominios, primero deberá decidir qué áreas harán intersección. Dichas áreas serán las que podrán participar en ambos dominios. Los números de esas áreas no se usarán en ningún otro lugar de los dos dominios.

La Figura 18 en la página 340 muestra que las áreas de intersección son las áreas 1 y 2. El resto de las áreas puede duplicarse en los dos dominios. En el ejemplo, hay dos áreas 3, 4 y 5 en cada dominio. Tenga en cuenta que nunca será posible permitir una conexión directa entre un nodo del área 3 del dominio A y uno del área 3 del dominio B. Lo mejor que puede hacer es dar a las áreas de intersección la posibilidad de hablar con partes de cada dominio.

Al diseñar la intersección, compruebe que ninguno de los dominios dependa de las rutas que atraviesan la intersección para mantener la conectividad entre áreas que no están en ésta. Como las rutas que entran y salen de la intersección se filtran, es probable que no tengan una posibilidad de alcance normal entre todas las áreas del dominio.

Para decidir cómo configurar los filtros de direccionamiento, establezca un mapa conciso de la configuración. En este mapa localice todas las áreas y trace el contorno de los dos dominios. A continuación, decida sobre la barrera de filtro que necesita establecer. Vaya siguiendo cuidadosamente la intersección de los dos dominios y localice todas las adyacencias de nivel 2 que atraviesan la barrera de filtro. Las adyacencias son vías de comunicaciones de un salto entre direccionadores de nivel 2 que cruzan entre áreas.

En el ejemplo hay seis adyacencias que cruzan la barrera, de 1.18 a 5.7, de 1.18 a 5.8, de 1.18 a 8.3, de 2.17 a 3.12, de 2.21 a 4.7 y de 2.21 a 4.9.

El primer paso para designar los filtros de áreas consiste en establecer filtros que eviten que las áreas de un dominio se propaguen al otro dominio. Las únicas rutas de áreas que deben dejar la intersección son aquellas que van a áreas de la intersección. En el ejemplo, son las áreas 1 y 2. Por consiguiente, sólo las rutas para las áreas 1 y 2 deben enviarse desde nodos como el 2.17 y el 3.12.

En los enlaces de punto a punto como 2.17 y 3.12, no es importante el punto que filtra, pero es probablemente más seguro filtrar en el punto de envío. Por consiguiente, habrá un filtro en la interfaz 2.17 que permita el reenvío únicamente de rutas de las áreas 1 y 2. Lo mismo se produce en las dos interfaces de 2.21 y el enlace entre 1.18 y 8.3.

Cuando el salto entre dos áreas sea una red Ethernet u otro soporte de difusión como 1.18 a 5.7 y 5.8, deberá tomar la decisión basándose en otras cuestiones. La mayoría de las redes Ethernet tienen la mayor parte de los nodos de direccionamiento de nivel 2 en un área y unos cuantos en la segunda área. En este caso, el filtro deberá estar en el área que tiene unos cuantos y no en la que tiene la mayoría. En el ejemplo, el nodo 1.18 es el agente foráneo de la red Ethernet en el área 5, por lo que debe filtrar. El nodo 1.18 debe enviar direccionadores únicamente para las áreas 1 y 2 de la red Ethernet.

Se puede filtrar en ambos extremos de una adyacencia. Esto permite añadir una capa adicional de seguridad contra las reconfiguraciones accidentales. No obstante, si sólo establece el filtro en un extremo, sólo dicho extremo filtrará.

Teniendo en cuenta estos filtros, los dos dominios no podrán contaminarse entre sí. No obstante, en el caso de un nodo de la intersección, no queda claro qué área 3 se alcanzará cuando intente establecerse una conexión con el nodo 3.4. Dependerá de la ruta actual y de los costos de circuito. Está claro que no se trata de una situación ideal. No importa que sólo haya un nodo 3.4 en el dominio A y ninguno en el dominio B. El direccionamiento entre áreas se efectúa únicamente basándose en el área; sólo los direccionadores de un área saben las rutas a los nodos de dicha área.

Por consiguiente, es necesario establecer otro conjunto de filtros para decidir qué instancia de un área (dominio A o B) podrá alcanzarse desde la intersección para cada área que no esté en la mencionada intersección. Puede decidir, por lo tanto, que los nodos de la intersección pueden llegar a las áreas 3 y 4 del dominio A y al área 5 del dominio B. En el ejemplo, esto puede efectuarse configurando los direccionadores 1.18 y 2.21 para que sólo acepten rutas a las áreas 3, 4, 6 y 8 del dominio A. Los direccionadores 2.17 y 2.21 sólo aceptarán rutas para las áreas 5 y 9 del dominio B.

Por consiguiente, los nodos de la intersección ven un universo que contiene las áreas 1 y 2 de la intersección, las áreas 3, 4, 6 y 8 del dominio A y las áreas 5 y 9 del dominio B.

Para configurar el direccionador 1.18 de la Figura 18 en la página 340, entre los parámetros y mandatos de NCP siguientes:

```
NCP> def mod routing-filter circ eth/0 outgoing area 1,2
NCP> def mod routing-filter circ eth/0 outgoing state on
NCP> def mod routing-filter circ eth/0 incoming area 3,4,6,8
NCP> def mod routing-filter circ eth/0 incoming state on
NCP> def mod routing-filter circ ppp/0 outgoing area 1,2
NCP> def mod routing-filter circ ppp/0 outgoing state on
NCP> def mod routing-filter circ ppp/0 incoming area 3,4,6,8
NCP> def mod routing-filter circ ppp/0 incoming state on
```

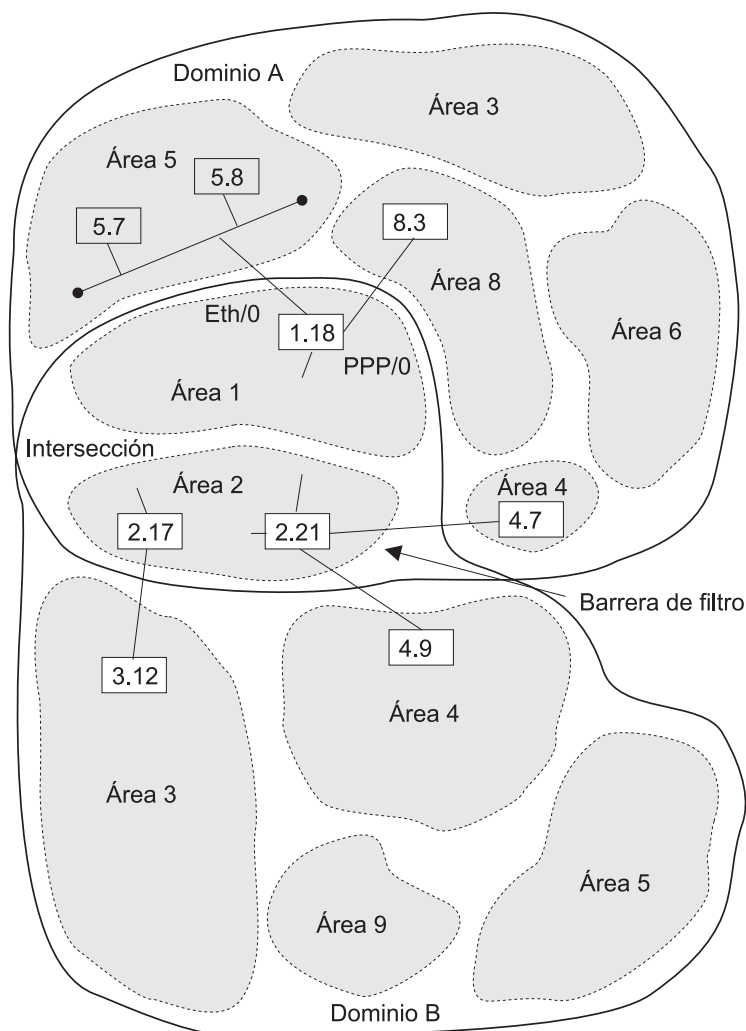


Figura 18. Ejemplo de fusión de dominios de DECnet

Sigue sin haber manera de que un nodo del dominio A área 5 pueda comunicarse directamente con un nodo del dominio B área 5. Para que los nodos de ambas áreas se comuniquen, deberá efectuar una serie de retardos de nivel de aplicación usando el mandato **set host**. Por ejemplo:

- Ejecute el mandato `set host` para iniciar sesión de forma remota desde un nodo del dominio A área 5 a otro nodo del dominio A área 8.
- Ejecute el mandato `set host` para iniciar sesión de forma remota desde un nodo del dominio A área 8 a otro nodo del área 1 ó 2.
- Ejecute el mandato `set host` para iniciar sesión de forma remota desde un nodo del área 1 ó 2 a otro nodo del dominio B área 5.

Configuración de DNA IV

El protocolo DNA IV se ejecuta sobre interfaces de red en anillo, Frame Relay, Ethernet, PPP, clientes de Token-Ring ATM LAN Emulation, clientes de Ethernet LAN Emulation clients y X.25. Las secciones siguientes describen los procedimientos para configurar el protocolo DNA IV para que funcione sobre interfaces de red en anillo y X.25.

Nota: Cuando se trabaje en redes DNA IV y DNA V mezcladas, toda la configuración y supervisión de DNA IV debe efectuarse en el proceso descrito en el presente capítulo.

Consideraciones del algoritmo de DNA IV y DNA V

DNA IV usa un algoritmo de direccionamiento de vector de distancia. DNA V puede usar un algoritmo de vector de distancia o bien un algoritmo de direccionamiento de estado de enlace. El algoritmo seleccionado por el direccionador de puenteo se establece de acuerdo con qué protocolo está habilitado o inhabilitado y las combinaciones que pueden producirse con estos dos protocolos. Consulte la Tabla 104 si desea ver más detalles.

Tabla 104. Consideraciones de algoritmo de DNA IV y DNA V

Estado de DECnet IV	Estado de OSI/DNA V	Algoritmo seleccionado
Habilitado	Inhabilitado	Vector de distancia (automáticamente)
Inhabilitado	Habilitado	Estado de enlace (automáticamente)
Habilitado	Habilitado	Use el mandato set algorithm para configurar esta información en la SRAM.

Configuración de DNA IV para red en anillo

El procedimiento para ejecutar el protocolo DNA IV sobre 802.5 Token Ring (TR) implica a mandatos de los procesos de configuración de DNA IV y la red en anillo.

- Desde el indicador OPCON (*) entre en el proceso de configuración.

```
* talk 6
Config>
```

- Entre **list device** para ver los números de interfaces para las interfaces de la red en anillo. Apunte el número de interfaz de cada interfaz de la red en anillo.

```
Config> list device
```

- Use el mandato **network** con el número de la interfaz de la red en anillo que desee configurar. Esto lo situará en el proceso de configuración de la red en anillo.

```
Config> network 0
TKR config>
```

- Use el mandato **list** para verificar la información de configuración de la red en anillo.

```
TKR config> list
```

```
Token-Ring configuration:
```

```
Packet size (INFO field): 2052
Speed: 4 Mb/sec
Media: Shielded
```

```
RIF Aging Timer: 120
Source Routing: Enabled
Mac Address 000000000000
```

- Salga del proceso de configuración de la red en anillo y entre en el de configuración de DNA NCP.

```
TKR config> exit
Config> protocol DN
NCP>
```

6. Use el mandato **define** para definir un circuito DNA en la interfaz de la red en anillo.

```
NCP> define circuit tkr/0 state on
```

7. Opcionalmente, use el mandato **define** para establecer el tipo de direccionamiento para el circuito. Para el soporte bilingüe o de Phase IV, deberá cambiar el tipo de direccionamiento y pasar del valor por omisión (estándar) a bilingüe o AMA.

```
NCP> define circuit tkr/0 router type bilingual
```

o-

```
NCP> define circuit tkr/0 router type AMA
```

8. Use el mandato **list** para comprobar los parámetros.

```
NCP> list circuit tkr/0 characteristics
Circuit Permanent Characteristics
Circuit           = TKR/0
State             = On
Cost              = 4
Router priority   = 64
Hello timer       = 15
Max routers       = 16
Router type       = Standard
```

9. Reinicie el direccionador para que todos los parámetros configurados entren en vigor.

Nota: Si desea inhabilitar el direccionamiento de origen o establecer el temporizador RIF en un valor que no sea el valor por omisión, use los mandatos **source-routing** y **set RIF-timer** en el proceso de configuración de la red en anillo.

Configuración de DNA IV para X.25

El procedimiento para ejecutar el protocolo DNA IV sobre circuitos X.25 implica a mandatos de los procesos de configuración de X.25 y DNA IV .

1. Desde el indicador OPCON (*) entre en el proceso de configuración. Vaya a "t 6" y entre X.25 config (# red). Si es la primera vez que configura X.25 haga lo siguiente:

- a. DEFINA la dirección DTE del direccionador.

```
X.25 Config> set address
```

- b. DEFINA cada protocolo que tendrá soporte sobre X.25:

```
X.25 Config> add protocol
```

IP Por lo general es buena idea añadir este protocolo para poder verificar si la configuración de X.25 general es correcta

DN

Nota: Permita que los parámetros del protocolo tomen los valores por omisión.

- c. DEFINA la correlación de la dirección remota del protocolo con la dirección X.25 remota para los protocolos que así lo requieran:

```
X.25 Config> add address
```

para IP:

- Dirección IP = 128.185.247.22
- Dirección X.25 = 22

para DN:

- Dirección DN = 5.22
- Dirección X.25 = 22

- d. VERIFIQUE que un extremo del circuito X.25 es un DTE y que el otro extremo es DCE.

```
X.25 Config> list all
```

Compruebe en el campo National Personality (Personalidad nacional) el tipo de dispositivo. En el caso del tipo de personalidad nacional de GTE-Telenet, verá:

```
National Personality: GTE Telenet (DTE)
```

-0-

```
National Personality: GTE Telenet (DCE)
```

Para cambiar el tipo de dispositivo a DCE, entre:

```
X.25 Config> set equipment-type dce
```

Listará todos los parámetros configurados para X.25

```
National Personality: GTE Telenet (DTE) National Personality: GTE Telenet (DCE)
```

Si no es así, elija un direccionador para que actúe como DCE y modifíquelo como tal,

```
X.25 Config> set national-personality dce
```

- e. REINICIE el direccionador para que todos los parámetros configurados entren en vigor.

- f. Para VERIFICAR que la configuración es válida después de un reinicio, vaya al lado del monitor y observe si el enlace se está activando.

```
* t
5
+ c
```

Esto le indicará el estado del enlace en ese momento. Si ve que el estado del enlace de X.25 pasa de "testing" a "down", vaya a los mensajes ELS y compruebe si se ha producido un error evidente. Si el estado del enlace de X.25 pasa de "testing" a "up", es muy posible que la configuración de X.25 sea válida.

2. Para VERIFICAR que el enlace de X.25 es operativo:

- a. INTENTE ejecutar un PING en cada extremo del enlace de X.25 desde el monitor de IP:

```
IP> interface
```

Verifique que se hayan configurado las direcciones de X.25 correctas en el protocolo IP.

```
IP> ping dirección IP del enlace X.25 remoto
```

3. Para CONFIGURAR DECnet PhaseIV en el direccionador:

- a. DEFINA los parámetros de DECnet Executor:

```
NCP> define exec address área.nodo Dirección DECnet del direccionador
```

NCP> **define exec type DEC-ROUTING-IV** Configura el direccionador como un direccionador de tipo LEVEL 1 DEC

Nota: Este ejemplo sirve para configurar un direccionador para que trabaje con otros direccionadores que dan soporte al estándar de direccionamiento DEC sobre redes X.25. Un direccionador que dé soporte al estándar debe definirse como tipo DEC-ROUTING-IV (nivel 1) o DEC-AREA (nivel 2). El tipo de direccionamiento por omisión es ROUTING-IV y AREA, lo que permite trabajar con varios IBM 2210 existentes y otros direccionadores compatibles.

NCP> **define exec state on**

Reinicie el direccionador para que cuando configure el circuito X.25, todos los parámetros específicos de DEC sean visibles. Para verificar la configuración del ejecutar, NCP> **show executor characteristics**

b. DEFINA circuitos de PhaseIV X.25.

Debe configurar el circuito X.25 como PVC o SVC. Si se configura este circuito como PVC, el otro extremo también tendrá que ser un PVC. Si se configura este circuito como un IN-SVC, el otro extremo deberá configurarse como un OUT-SVC

```
NCP> define cir x25/0 usage IN-SVC
NCP> define cir x25/0 DTE-address "remote X.25 DTE"
NCP> define cir x25/0 call-data
NCP> define cir x25/0 verification enabled
```

La habilitación de la verificación es opcional.

c. DEFINA circuitos en el estado activo:

- para la red en anillo

```
NCP> define cir TKR/0 router type bilingual
```

- para TODOS los circuitos

```
NCP> define cir xxx state on
```

Reinicie el direccionador para que todos los parámetros de DECnet entren en vigor, VERIFIQUE que la configuración de X.25 en el protocolo DECnet es tal como la desea.

```
NCP> list circuit x25/0 characteristics
```


Configuración y supervisión de DNA IV

Mandatos de configuración y supervisión de DNA IV

Esta sección describe los mandatos de supervisión y configuración de NCP. Entre los mandatos en el indicador NCP>. Puede accederse a **todos** los mandatos de NCP desde los entornos de configuración o de supervisión.

Tabla 105. Mandatos de configuración y supervisión de NCP

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte la sección "Cómo obtener ayuda" en la página xxix.
define	Define elementos de la base de datos no volátil (permanente), incluidos: <ul style="list-style-type: none"> • Listas de control de acceso y filtros de direccionamiento • Elementos de circuitos • Argumentos globales para DNA • Datos de configuración de los nodos
purge module	Elimina listas de control de acceso y filtros de direccionamiento de la base de datos permanente.
set	Establece o cambia elementos de la base de datos volátil, incluidos: <ul style="list-style-type: none"> • Elementos de circuitos • Argumentos globales para DNA • Datos de configuración de los nodos
show	Muestra el estado de la base de datos volátil y nodos volátiles de la base de datos de direccionamientos.
show/list	Muestra elementos de la base de datos volátil (show) o permanente (list), incluyendo: <ul style="list-style-type: none"> • El estado actual de los circuitos especificados • El estado actual de la base de datos volátil/permanente para DNA • Las listas de control de acceso de DECnet que se han definido en la base de datos permanente para el direccionador • Los filtros de direccionamiento de áreas de DECnet que se han definido en la base de datos permanente para el direccionador
zero	Borra los contadores de circuito de la base de datos volátil, los contadores globales de la base de datos volátil y los contadores del módulo de la lista de control de acceso. <i>No borra los valores de los argumentos establecidos con los mandatos set o define.</i>
Exit	Le devuelve al nivel de mandatos anterior. Consulte la sección "Cómo salir de un entorno de nivel inferior" en la página xxix.

Tenga en cuenta la información siguiente sobre los mandatos:

1. Los mandatos **define** no entran en vigor hasta la siguiente vez que se inicia el direccionador.
2. Los mandatos **list**, **define** y **purge** modifican o muestran datos en la base de datos permanente (RAM estática del direccionador). La base de datos permanente se almacena en la configuración y se aplica en todos los reinicios, cargas de software y ciclos de alimentación.
3. Los mandatos **show** y **list** son los más útiles para supervisar el protocolo DNA IV.
4. Use **set**, **show** y **zero** para modificar, visualizar o borrar datos de la base de datos volátil.
5. El mandato **zero** borra las estadísticas guardadas en la base de datos volátil, pero **no** borra los valores de argumento establecidos con los mandatos **set** o **define**.

Define/Set

Esta sección explica los mandatos **define** y **set**.

Use el mandato **define** para definir listas de control de accesos y filtros de direccionamiento y para definir parámetros de circuito, ejecutor y nodo. **Define** se usa para establecer la SRAM (necesita un reinicio).

Sintaxis:

```
define          circuit-specifier . . .  
                executor . . .  
                module access-control . . .  
                module routing-filter . . .  
                node . . .
```

Set puede usarse para la RAM volátil (cambio inmediato, no es necesario un reinicio).

Sintaxis:

```
set           circuit-specifier . . .  
                executor . . .  
                node . . .
```

circuit-specifier *argumento*

Las opciones de *circuit-specifier* incluyen:

active circuits

Especifica todos los circuitos que están activos y cuyo estado sea on (activo) (únicamente para set).

all circuits

Especifica todos los circuitos del direccionador.

circuit name

El nombre del circuito. Por ejemplo: Eth/0, TKR/0, PPP/1.

known circuits

(únicamente **set**) Especifica todos los circuitos del direccionador.

Los *argumentos* incluyen:

call-userdata

Se usa durante la inicialización de los circuitos X.25 estáticos. Cuando se define un circuito como SVC de salida, las solicitudes de llamada inicial y posteriores contienen los datos de usuario de llamada definidos al habilitar el circuito. Cuando se define un circuito como SVC de entrada, uno de los criterios seguidos para aceptar una solicitud de llamada de entrada es una coincidencia de los datos del usuario de llamada definidos.

Actualmente los datos del usuario de llamada deben establecerse en el DTE del direccionador local para los SVC de llegada y de salida.

Entre un número par de caracteres hexadecimales (octetos) que tenga un máximo de 14 caracteres.

cost [rango]

Establece el coste de la recepción de un paquete en este circuito. Lo usa el algoritmo de direccionamiento para determinar el coste de un circuito al elegir rutas (el coste no es lo mismo que una métrica de IP). Rango: De 1 a 25. Valor por omisión: 4.

Los valores siguientes son puntos de inicio sugeridos:

<i>Tipo de circuito</i>	<i>Coste</i>
Ethernet	4
Red en anillo 4/16	4
Sync 56 Kb	6
Sync T1	5
X.25	25

Ejemplo:

```
define circuit tkr/0 cost 5
```

DTE Address

Especifica la dirección del DTE remoto del circuito X.25. Se trata siempre de la dirección del sistema remoto. Es un número decimal con un máximo de 14 caracteres.

hello timer [rango]

Especifica la frecuencia (en segundos) con la que se envían hellos del direccionador en este circuito. Rango: De 1 a 8191 segundos. Valor por omisión: 15 segundos (recomendado).

maximum recalls

(sólo **define**) Especifica cuántos intentos debe hacer el direccionador para volver a establecer una llamada de un SVC estático de salida después de un fallo inicial de la

llamada. Después de alcanzar el número máximo de rellamadas, el direccionador ya no efectúa ningún intento de establecer el SVC sin la intervención del usuario. Los valores válidos están en el rango incluido entre 1 y 20; el valor por omisión es 1. Consulte también el argumento `recall timer`.

maximum routers [rango]

(sólo **define**) Especifica cuántos direccionadores más puede haber en este circuito. Rango: De 1 a 33. Valor por omisión: 16.

Nota: El usuario no puede configurar este parámetro en un circuito X.25 cuando el *tipo* de ejecutor se establece en DEC-routing-IV o DEC-area. En dicho caso, el número máximo de direccionadores es 1.

Si se trata de un direccionador de nivel 1, sólo cuentan los direccionadores de este circuito de la misma área. Si se trata de un direccionador de nivel 2, cuentan todos los direccionadores de este circuito. El direccionador local no cuenta en relación con el límite.

Los requisitos de memoria y eficacia del direccionador mejoran manteniendo bajo este número. Establezca este argumento en valor algo superior al número total de direccionadores adyacentes en el circuito. No lo establezca en un valor inferior al número de direccionadores del circuito; pueden producirse anomalías en el direccionamiento.

Nota: En el caso de un circuito de punto a punto (línea síncrona), establezca este argumento en 1. Conseguirá obtener ahorros significativos de memoria en un direccionador con varias líneas de punto a punto.

La suma del número máximo de direccionadores sobre los circuitos debe ser inferior al argumento del número máximo de los direccionadores de difusión, aunque este límite no se aplica con rigurosidad.

recall timer

Determina el retardo, en segundos, entre los intentos de llamada para establecer un circuito estático de salida X.25.

Para **define**, los valores válidos están en el rango incluido entre 1 y 60 segundos. El valor por omisión es 1 segundo. Consulte también el argumento `maximum recalls`.

Para **set**, los valores válidos están en el rango incluido entre 0 y 65595. El valor por omisión es 60 segundos.

router priority [rango]

Especifica la prioridad del direccionador en las solicitudes para convertirse en el direccionador de los nodos finales de este circuito. Rango: De 1 a 127, donde 127 es la mayor prioridad. Valor por omisión: 64.

Si dos direccionadores tienen la misma prioridad, aquel que tenga la dirección de nodo más elevada ganará. La prioridad de direccionador no influye en las decisiones de

direccionamiento de área o cuando se intenta alcanzar el direccionador de nivel 2 conectado más cercano.

Utilice la prioridad de direccionador para elegir el direccionador designado para que sea el que tenga más probabilidades de convertirse en el mejor salto siguiente de los nodos finales del circuito. Si un circuito tiene dos direccionadores, uno de ellos con 500 nodos tras él y el otro con 20, el que tenga los 500 nodos deberá tener mayor prioridad de direccionador. No obstante, esto no es obligatorio, ya que una vez que un paquete de un nodo final alcance un direccionador, será reenviado a su destino.

Este argumento es irrelevante en las líneas de punto a punto, donde no hay nodos finales. (De todas maneras se selecciona un direccionador designado).

router type

Especifica el tipo de direccionamiento que debe efectuar el direccionador: **standard** (estándar), **AMA** o **bilingual** (bilingüe).

- *Standard*. Especifica que el direccionador está usando el direccionamiento phase IV convencional donde la dirección del MAC se crea a partir del número de nodo y de área. El direccionador tiene como valor por omisión este tipo.

- *AMA*. Especifica que el direccionador puede direccionar paquetes que usan el direccionamiento phase IV donde la dirección del MAC es arbitraria y se sabe por la capa de enlace de datos.

- *Bilingual*. Especifica que el direccionador puede direccionar paquetes que usan el direccionamiento convencional y phase IV con AMA.

state

Cuando se establece en **on**, especifica que el circuito está habilitado para que lo use DNA. Cuando se establece en **off**, especifica que el circuito está inhabilitado para que lo use DNA. **off** es el valor por omisión.

usage

Especifica si un circuito X.25 es:

- **PVC**: Un circuito virtual permanente
- **OUT-SVC**: Un circuito estático de salida
- **IN-SVC**: Un circuito estático de entrada

Este parámetro se aplica cuando el tipo de ejecutor está establecido en *DEC-routing-IV* o *DEC-area*. (Consulte **circuit executor type** para obtener más información).

verification

Especifica si el direccionador compara una serie de caracteres de verificación en el direccionador, en los datos de verificación de un mensaje de inicialización de entrada. Si no coinciden, deberá reinicializarse el circuito X.25. Debe especificar **enabled** (habilitado) o **disabled** (inhabilitado).

executor *argumento*

Define o establece argumentos (es decir, el ejecutor) globales para DNA en la base de datos permanente (**define**) o volátil (**set**).

La mayoría de estos argumentos reducen la eficacia del direccionador y aumentan la carga en los circuitos, ya que se amplían. También pueden aumentar los requisitos de memoria. No deben exceder los valores necesarios para la configuración de red actual.

Para **set**, el ejecutor debe estar desactivado para modificar los argumentos numéricos o escribir en la base de datos volátil. (A diferencia de DECnet-VMS, el mandato **set executor state on** es válido cuando el estado del ejecutor esté desactivado). Estos cambios se producen inmediatamente sin que sea necesario reiniciar el direccionador.

address [área.nodo]

Establece la dirección de nodo del ejecutor, el ID de nodo de este direccionador. Rango de área: De 1 a 63. El área y el nodo deben ser inferiores al área máxima del ejecutor. El rango de nodo está incluido entre 1 y 1023. El valor por omisión 0.0 es ilegal.

Nota: DNA no se habilitará si la dirección del ejecutor no se establece en un valor legal.

area maximum cost [número]

El costo máximo permitido entre este direccionador de nivel 2 y cualquier otro direccionador de nivel 2. Si la mejor ruta a un área es más costosa que este valor, se considerará que dicha área no se puede alcanzar. Máximo: 1022. Valor por omisión: 1022. Este argumento no se aplica a los direccionadores de nivel 1. Debería ser superior al costo legal máximo al área más distante. Se sugiere el valor "area maximum hops" multiplicado por 25.

area maximum hops [número]

Número máximo de saltos permitidos entre este direccionador de nivel 2 y cualquier otro direccionador de nivel 2. Si la mejor ruta a un área requiere más saltos que los indicados, se considerará que dicha área no se puede alcanzar. Máximo: 30. Valor por omisión: 30. Este argumento no se aplica a los direccionadores de nivel 1. Debería ser el doble de la longitud de vía de acceso más larga (en saltos) de lo que se espera.

El direccionamiento usa la cuenta de saltos únicamente para acelerar el abandono de rutas a las áreas que son inaccesibles. Area maximum hops puede reducirse para que las áreas que no son accesibles se conviertan en inaccesibles con mayor rapidez.

broadcast routing timer [rango]

Especifica la frecuencia de envío, en segundos, de los mensajes de nivel 1 (y 2 en un direccionador de nivel 2). Indica la frecuencia con la que se enviarán en ausencia de cualquier cambio de costo o adyacencia. Este parámetro sirve para proteger la base de datos de direccionamientos contra la corrupción. Si algún costo o adyacencia cambia, se envían

automáticamente, como mínimo, actualizaciones parciales de direccionamiento. Rango: De 1 a 65535. Valor por omisión: 180. Los valores inferiores aumentan la actividad general de este direccionador así como la del resto de los direccionadores adyacentes. Los valores más grandes aumentan el tiempo necesario para corregir la base de datos de direccionamientos si se pierde un mensaje de actualización parcial de direccionamientos.

maximum address number [rango]

(sólo **define**) La dirección de nodo más grande (dentro de esta área) para la que este direccionador mantendrá rutas. La base de datos de direccionamientos no incluirá rutas a nodos de esta área cuya parte de nodo sea superior a la dirección. Rango: De 1 a 1023. Valor por omisión: 32. Debe ser superior a la dirección de nodo más grande del área del direccionador. Si el valor que establece es demasiado grande, esto influirá en la eficacia del direccionador y utilizará una cantidad excesiva de memoria. Este argumento no entrará en vigor hasta que se reinicie el direccionador.

maximum area number [número]

(sólo **define**) El área superior para las que se mantendrán rutas, si se trata de un direccionador de nivel 2. La base de datos de direccionamientos no incluirá rutas a áreas superiores a esta. Máximo: 63. Valor por omisión: 63. Debe ser superior al número de área superior de toda la red. Este argumento no entrará en vigor hasta que se reinicie el direccionador.

maximum broadcast nonrouters [número]

(sólo **define**) Número máximo de nodos finales que pueden ser adyacentes (a un salto) de este direccionador. Se trata de la suma de todos los circuitos de difusión. Si hay más nodos finales, este direccionador no podrá alcanzar algunos de ellos, lo cual puede provocar problemas de direccionamiento imprevisibles. Este argumento no entrará en vigor hasta que se reinicie el direccionador. Rango: De 1 a 1023. Valor por omisión: 63.

maximum broadcast routers [número]

(sólo **define**) Número máximo de direccionadores que pueden ser adyacentes (a un salto) de este direccionador. Se trata de la suma de todos los circuitos de difusión. Si hay más direccionadores, no se aceptarán las rutas de los direccionadores sobrantes. Esto puede provocar problemas de direccionamiento imprevisibles. Este argumento no entrará en vigor hasta que se reinicie el direccionador. Valor por omisión: 32. Máximo: el número de circuitos multiplicado por 33. Este valor debe ser superior o igual a la suma de "circuit maximum routers" de todos los circuitos, aunque este punto no se aplique con rigurosidad. Este parámetro tiene una gran influencia en la utilización de la memoria y no debe establecerse en un valor que sea demasiado superior al necesario. Dado que el valor por omisión es bastante alto, es

posible que tenga que reducirlo si ha establecido el parámetro "maximum address" en un valor también alto.

maximum cost [número]

El costo máximo permitido entre este direccionador y cualquier otro nodo del área. Si la mejor ruta a un nodo es más costosa que este valor, se considerará que dicho nodo no se puede alcanzar. Máximo: 1022. Valor por omisión: 1022. Debería ser superior al costo legal máximo al nodo más distante. Se sugiere el valor del parámetro "maximum hops" multiplicado por 25.

maximum hops [número]

Número máximo de saltos permitidos entre este direccionador y cualquier nodo del área. Si la mejor ruta a un nodo requiere más saltos que los indicados, se considerará que dicho nodo no se puede alcanzar. Máximo: 30. Valor por omisión: 30. Debería ser el doble de la longitud de vía de acceso más larga (en saltos) de lo que se espera. El direccionamiento usa la cuenta de saltos únicamente para acelerar el abandono de rutas a nodos que son inaccesibles. El parámetro maximum number of hops puede reducirse para que los nodos que son inaccesibles se conviertan en inaccesibles con mayor rapidez.

maximum visits [número]

Especifica que cualquier paquete que este direccionador reenvíe y que se haya reenviado más veces de las indicadas en el parámetro de los direccionadores de número máximo de visitas, se eliminará. Se usa para detectar paquetes que están en bucles de direccionamiento, lo que se produce cuando las rutas se abandonan. El número máximo de visitas es 63. Este es el valor por omisión. Este argumento debe ser superior, en un valor al cuadrado, a los parámetros maximum hops y area maximum hops.

state on Habilita DNA. Puede emitirse en cualquier momento, siempre y cuando el direccionador tenga una dirección de nodo válida.

state off Inhabilita DNA. Puede emitirse en cualquier momento. El estado por omisión es off (desactivado).

En el caso de **set**, **set executor** se inhibirá si la inicialización de DNA falló debido a falta de memoria disponible para las tablas de direccionamiento.

type (sólo **define**) En los circuitos X.25, provoca que el direccionador actúe según una de las cuatro maneras siguientes, según el valor seleccionado. Las opciones son:

DEC-routing-iv

configura el direccionador como un direccionador de nivel 1 compatible con DEC.

DEC-area

configura el direccionador como un direccionador de nivel 2 (área) compatible con DEC.

Routing-iv

configura el direccionador como un direccionador de nivel 1 sin compatibilidad con DEC en los circuitos X.25. Este es el valor por omisión.

Area configura el direccionador como un direccionador (área) de nivel 2 sin compatibilidad con DEC en los circuitos X.25.

Un direccionador de nivel 2 acepta las adyacencias con direccionadores de otras áreas y mantiene rutas a todas las áreas. Si puede llegar a otras áreas, también se anuncia a los direccionadores de nivel 1 como una ruta a otras áreas.

En el caso de los direccionadores de nivel 1, se aceptan únicamente las adyacencias con otros direccionadores de la misma área.

Ejemplo: define executor state on

```
define executor type DEC-area
```

```
define executor maximum broadcast routers 10
```

type area (sólo **set**) Hace que el direccionador actúe como un direccionador de nivel 2. Este direccionador aceptará las adyacencias con direccionadores de otras áreas y mantendrá rutas a todas las áreas. Si puede llegar a otras áreas, también se anunciará como ruta a otras áreas a los direccionadores de nivel 1.

El estado de DNA debe estar establecido en *off* antes de cambiar el *tipo*.

type routing-IV

(sólo **set**) Hace que el direccionador actúe como un direccionador de nivel 1, que es el valor por omisión. Las adyacencias sólo se aceptarán para las rutas de la misma área.

El estado de DNA debe estar establecido en *off* antes de cambiar el *tipo*.

Ejemplo: set executor state on

```
set executor maximum broadcast routers 10
```

module access-control *argumento especificador de circuito*

(sólo **define**) Define las listas de control de acceso que se usan para restringir el reenvío de paquetes entre algunos orígenes y destinos. Cada lista de acceso se asocia a un circuito y se aplica a los paquetes de datos de formato largo de DECnet recibidos en dicho circuito. El control de acceso no se aplica a ningún paquete hello o de direccionamiento.

Los argumentos para los especificadores de circuitos incluyen:

all circuits

Especifica todos los circuitos del direccionador.

circuit name

Especifica el circuito nombrado.

known circuits

Especifica todos los circuitos del direccionador.

Los elementos siguientes son argumentos que puede seleccionar después de entrar el mandato **define module access-control** y el especificador de circuito:

state on Habilita la lista de control de acceso en este circuito.

state off Inhabilita la lista de control de acceso en este circuito.

type exclusive

Especifica que los paquetes que coincidan con uno o varios filtros de la lista de control de acceso de esta interfaz se eliminarán.

type inclusive

Especifica que sólo los paquetes que coincidan con uno o varios filtros de la lista de control de acceso de esta interfaz se reenviarán.

filter [resultado-origen máscara-origen resultado-destino máscara-destino]

Añade un filtro a la lista del circuito especificado. Se añade el filtro al final de la lista existente.

Se enmascara la dirección de origen con la máscara de origen y se compara con el resultado del origen. Lo mismo se hace con la máscara de destino y el resultado de destino. La acción dependerá del tipo de control de acceso que se use en el circuito.

Los elementos siguientes son las opciones en las que selecciona después de entrar el mandato **define module access-control** y el especificador de circuitos **filter**:

source-result

Dirección con la que se compara la dirección de origen después de enmascararla.

source-mask

Máscara usada para la dirección de origen.

dest-result

Dirección con la que se compara la dirección de destino después de enmascararla.

dest-mask

Máscara usada para la dirección de destino.

Ejemplo: define module access-control circuit eth/0 state on

module routing-filter *argumento especificador de circuito*

(sólo **define**) Define los filtros de direccionamiento que se usan para restringir el envío de rutas de área por direccionadores de nivel 2 (Executor Type Area).

all circuits

Especifica todos los circuitos del direccionador.

circuit name

Especifica el circuito nombrado.

known circuits

Especifica todos los circuitos del direccionador.

Los elementos siguientes son las opciones de dirección que selecciona después de entrar el mandato **define module routing-filter** y el especificador de circuitos:

incoming Influye en el filtro de información de direccionamiento recibido en este circuito.

outgoing Influye en el filtro de información de direccionamiento enviado en este circuito.

Los elementos siguientes son los argumentos que selecciona después de entrar el mandato **define module routing-filter** y el especificador de circuitos:

area [lista áreas]

Especifica que el filtro permite que la información de direccionamiento pase por el conjunto de áreas establecido en la lista de áreas. La lista de áreas es una lista de áreas o rangos de áreas separadas por comas. Los rangos se especifican con dos números de área separados por un guión. La lista de áreas puede no tener ningún contenido, con lo que se especifica que la información no se pasará a ninguna área. A continuación se muestran ejemplos de listas de áreas:

1,4,9,60 Áreas 1, 4, 9 y 60

1-7,9-13,23

Áreas 1, 2, 3, 4, 5, 6, 7, 9, 10, 11, 12, 13 y 23

state on Especifica que el filtro está activo.

state off Especifica que se ha inhabilitado el filtro pero que continúa almacenado en la base de datos permanente. La única forma de sacar el filtro consiste en usar el mandato **purge**.

Ejemplo: define module routing-filter circuit eth/0 state on

node argumento

Permite definir o establecer información de configuración en nodos de la base de datos volátil (**set**) o permanente (**define**). El único nodo del que se mantiene información es el nodo ejecutor, ya que los nombres de nodo no se almacenan. El nodo especifica la dirección de nodo del direccionador (del ejecutor). Consulte la descripción del mandato **define executor**.

Ejemplo: define node state on

Ejemplo: set node state on

Purge

Use el mandato **purge** para eliminar listas de control de acceso y filtros de direccionamiento de la base de datos permanente.

Sintaxis:

purge module access-control . . .

Mandatos de configuración y supervisión de DNA IV

module routing-filter . .

module access-control *especificador de circuito*

Elimina listas de control de acceso de la base de datos permanente.
Puede suprimir una lista de control de acceso completa; no se puede suprimir un filtro.

all circuits

Especifica todos los circuitos del direccionador.

circuit name

Especifica el circuito nombrado.

Ejemplo: purge module access-control all circuits

module routing-filter *especificador de circuito*

Elimina filtros de direccionamiento de la base de datos permanente.
Puede depurar un filtro especificado o bien depurarlos todos.

Las opciones para los especificadores de circuitos son las siguientes:

all Especifica todos los filtros de direccionamiento de la memoria de configuración.

circuit name

(Nombre circuito) Especifica el filtro de direccionamiento del circuito nombrado.

Ejemplo: purge module routing-filter all

Set

Use el mandato **set** para añadir, establecer o modificar especificadores de circuito, argumentos globales, módulos de enlace de datos o nodos de la base de datos DNA volátil.

Sintaxis:

```
set          circuit . . .  
             executor . . .  
             node . . .
```

Para leer una descripción de estas opciones, Consulte "Define/Set" en la página 346.

Show

Use el mandato show para mostrar el estado de la base de datos volátil y los nodos volátiles de la base de datos de direccionamientos.

Sintaxis:

```
show        area-specifier . . .  
             node-specifier . . .
```

area-specifier *argumento*

Examina el estado de la base de datos de direccionamientos de área volátil. Esto le permite saber qué áreas puede alcanzar y qué rutas hay para las diferentes áreas.

Las opciones para los especificadores de área son las siguientes:

active areas

Proporciona información sobre las áreas que se pueden alcanzar actualmente.

all areas Proporciona información sobre todas las áreas (hasta el área máxima del ejecutor).

area Proporciona información sobre el área especificada. Si no indica el área, se le solicitará que la indique.

known areas

Proporciona información sobre las áreas que se pueden alcanzar actualmente.

Los elementos siguientes son las opciones de submandato que puede seleccionar después de entrar el mandato **show** y el especificador de área:

characteristics

Muestra el estado actual del área especificada. (Lo mismo que summary).

status Proporciona información detallada sobre las áreas especificadas, incluyendo el costo y los saltos.

summary Muestra el estado actual de las áreas especificadas. Este es el valor por omisión.

Ejemplo.: show active areas

```
Active Area Volatile Summary
Area State      Circuit Next
                Node
1  reachable    Eth/0  1.22
2  reachable    2.26
3  reachable    X25/0  2.30
```

Ejemplo: show active areas status

```
Active Area Volatile Status
Area State      Cost Hops Circuit Next
                Node
1  reachable    3   1   Eth/0  1.22
2  reachable    0   0     2.26
3  reachable    2   1   PPP/0  3.9
6  reachable   12  3   PPP/0  3.9
3  reachable   11  1   X25/0  2.30

Area Volatile Status
Area State      Cost Hops Circuit Next
                Node
5  unreachable 1023 31
```

Los elementos siguientes definen la información que aparece cuando usa el mandato **show**.

area (área) Indica el área de esta línea de la pantalla.

circuit (Circuito) Indica a qué circuito irá el salto siguiente a este nodo. No se da ningún circuito para el área propia del direccionador.

cost (Costo) Indica el costo a esta área.

hops (Saltos) Indica los saltos a esta área.

next node

(nodo siguiente) Indica qué direccionador será el salto siguiente (destino intermedio) al área especificada.

state (estado) Indica si se podrá alcanzar o no.

node-specifier *argumento*

Muestra el estado de la base de datos de direccionamientos de nodos volátil; se incluye información sobre los nodos que pueden alcanzarse y cuáles son las rutas que llevan hacia ellos.

Los especificadores de nodo pueden ser uno de los especificadores siguientes:

active nodes

Proporciona información sobre todos los nodos que pueden alcanzarse actualmente.

all nodes Proporciona información sobre todos los nodos (hasta la dirección máxima del ejecutor). Una visualización de todos los nodos incluye información sobre el "pseudomodo" área.0. Cualquier direccionador de nivel dos que alcance otras áreas anunciará la ruta al área.0 de nodo. Los direccionadores de nivel uno usan estas rutas para reenviar todos los paquetes al direccionador de nivel uno más cercano que sepa cómo llevar el paquete al área correcta. No existe otra manera de examinar el nodo 0, ya que no se trata de una dirección de nodo legal.

node node

Proporciona información sobre el nodo especificado. Si no se indica el nodo, se le solicitará que lo indique.

known nodes

Proporciona información en los nodos que se pueden alcanzar en la actualidad.

Los argumentos incluyen:

characteristics/ summary

Ambas opciones de submandatos muestran el estado actual de los nodos especificados.

status Proporciona información detallada sobre los nodos especificados, incluyendo el costo y los saltos.

Ejemplo: show node status

Este ejemplo muestra el estado detallado de un nodo específico.

```
Which node [1.9]? 2.26
Node Volatile Status
Executor node      = 2.26 (gato)
State             = on
Physical address   = AA-00-04-00-1A-08
Type              = DEC-area
```

Ejemplo: show active nodes

Este ejemplo muestra los nodos que se pueden alcanzar.

```
Active Node Volatile Summary
Executor node      = 2.26 (gato)
State             = on
Identification     = DECnet-MC68360 V1 R2.0 NP00523
[P10]

Node   State   Circuit Next
Address
2.14  reachable Eth/0  2.14
2.34  reachable PPP/0  2.34
2.37  reachable PPP/0  2.34
1.22  reachable Eth/0  1.22
```

Ejemplo: show adjacent nodes status

Este ejemplo muestra información de direccionamiento detallada sobre todos los nodos adyacentes. Sólo se mostrarán los nodos que tengan un salto. Sólo se sabe y se muestra el tipo de nodo de los nodos adya-

centes ya que esta información sólo está contenida en los mensajes hello.

```
Adjacent Node Volatile Status
Executor node      = 2.26 (gato)
State              = on
Physical address   = AA-00-04-00-1A-08
Type               = DEC-area
Node      State   Type      Cost   Hops  Circuit  Next
Addr
2.14  reachable routing IV    3     1   Eth/0   2.14
2.34  reachable routing IV    2     1   PPP/0   2.34
2.42  reachable nonrouting IV  2     1   PPP/0   2.42
1.22  reachable  area          3     1   Eth/0   1.22
```

Show/List

Use el mandato **show circuit** para recuperar información sobre el estado actual de los circuitos especificados de la base de datos volátil. El mandato **list circuit** recupera los datos almacenados en la base de datos permanente para los circuitos.

Sintaxis:

```
show      all
          area
          circuit . . .
          executor . . .
          known argumento
          module argumento
          node argumento
```

Sintaxis:

```
list      all
          area
          circuit argumento
          executor argumento
          module
          node argumento
```

circuit-specifier *argumento*

Las opciones de los especificadores de circuito son las siguientes:

active circuits

Especifica todos los circuitos que están actualmente activados (por base de datos volátil).

all circuits

Especifica todos los circuitos del direccionador.

circuit name

(nombre circuito) Especifica el circuito nombrado.

known circuits

Especifica todos los circuitos del direccionador.

Los elementos siguientes son las opciones de submandato que selecciona después de entrar el mandato y el especificador de circuito:

characteristics

Proporciona información detallada sobre todos los valores de argumentos para el circuito.

counters Muestra los contadores del circuito.

status Muestra información detallada sobre el circuito de la base de datos volátil.

summary Muestra información resumida sobre el circuito de la base de datos volátil. Se trata del valor por omisión si no se proporciona ningún argumento.

Ejemplo: show all circuits

```
Circuit Volatile Summary
Circuit State      Adjacent
                  Node
X25/0  on          5.25
Eth/0   on          1.22
Eth/0   on          2.14
Eth/0   on          1.13
PPP/0   off
```

Ejemplo: list circuit eth/0 characteristics

```
Circuit Permanent Characteristics
Circuit              = Eth/0
State                = On
Cost                 = 4
Router priority     = 64
Hello timer         = 15
Maximum routers     = 16
Router type         = Standard
```

Ejemplo: show active circuits status

```
Active Circuit Volatile Status
Circuit State      Adjacent  Block
                  Node      Size
Eth/0   on          1.22   1498
Eth/0   on          2.14   1498
Eth/0   on          1.13   1498
X25/0   on          5.25   1498
```

Ejemplo: show all circuits characteristics

Este ejemplo muestra las características actuales de los circuitos de esta máquina. Esto incluye todos los argumentos de la configuración, así como las adyacencias actuales y el temporizador de escucha (el temporizador hello de la adyacencia multiplicado por tres).

```
Circuit Volatile Characteristics
Circuit              = Eth/0
State                = on
Designated router   = 2.26
Cost                 = 4
Router priority     = 64
Hello timer         = 15
Maximum routers     = 16
Adjacent node       = 1.22
Listen timer        = 45
Adjacent node       = 2.14
Listen timer        = 45
Adjacent node       = 2.39
Listen timer        = 90
Circuit              = PPP/0
State                = off
Designated router   =
Cost                 = 4
Router priority     = 64
Hello timer         = 15
Maximum routers     = 8
```

Ejemplo: show circuit eth/0 counters

Este ejemplo muestra los contadores que existen para los circuitos. Tenga en cuenta que algunos de los contadores que DECnet-VAX lleva no están aquí, sino que se leen con el mandato **network** de GWCON.


```
Circuit Volatile Counters
Circuit = Eth/0
525249 Seconds since last zeroed
0 Terminating packets received
0 Originating packets sent
3693 Transit packets received
4723 Transit packets sent
0 Transit congestion loss
0 Circuit down
0 Initialization failure
0 Packet corruption loss
```

adjacent node

ID de un nodo con una adyacencia con este nodo en el circuito que se está mostrando. Mientras que las adyacencias con nodos finales convierten a dicho nodo en automáticamente accesible, una adyacencia de direccionador no convierte automáticamente en accesible a dicho nodo. No se considera que un direccionador es accesible a menos que se haya recibido un mensaje de direccionamiento sobre una adyacencia activa del direccionador. Por consiguiente, los nodos pueden aparecer como adyacentes en la base de datos de circuitos pero no estarán en la base de datos de nodos accesible (show active nodes).

block size

Tamaño máximo del bloque de datos que está dispuesto a recibir el nodo adyacente asociado. Por lo general, el tamaño es de 1498 bytes, que es el estándar de 1500 bytes de un paquete Ethernet, menos el campo de longitud de 2 bytes usado con DECnet.

circuit Circuitos en los que se aplican estos datos.

designated router

Muestra cuál cree, este nodo, que es el direccionador designado para esta área en este circuito. (Puede haber algunos desacuerdos temporales cuando se inicia un direccionador nuevo). Por lo general será el mismo para todos los direccionadores del circuito. Los nodos finales envían todos los paquetes que van a destinos que no están en el circuito local al direccionador designado.

hello timer

Temporizador hello de este circuito. Los mensajes hello del direccionador se envían a menudo al circuito.

listen timer

Período de tiempo que designa la frecuencia con que deben recibirse los hellos de nodos finales o de direccionadores de esta adyacencia en este circuito. El valor será el tiempo establecido para el temporizador hello para este circuito en la máquina adyacente, multiplicado por tres.

router priority

Prioridad de direccionador para este circuito, que se usa para conseguir el estado de direccionador designado.

router type

Tipo de direccionador para este circuito - standard (estándar), phase IV con AMA o Bilingual (bilingüe).

maximum routers

Número máximo de direccionadores permitido en este circuito.

state

ON u OFF. En la base de datos volátil, el estado será ON si se habilita el circuito y está pasando una autoprueba. Si el circuito ha fallado en la autoprueba o el dispositivo no está presente, el estado será OFF.

En la base de datos permanente, indica si DNA intentará habilitar el circuito.

executor *argumento*

Recupera información sobre el estado actual de la base de datos volátil para DNA con el mandato show executor. El mandato **list executor** recupera los datos almacenados en la base de datos permanente para DNA.

A continuación, se muestra una lista de las opciones de submandato o argumentos que puede seleccionar después de entrar el mandato show/list executor:

characteristics

Información detallada sobre los valores de todos los argumentos ajustables de la base de datos de direccionamientos.

counters Indica los contadores de errores y de sucesos globales para DNA. No hay contadores permanentes, por lo que el mandato **list executor counters** es irrelevante.

status Da información clave sobre el estado de DNA.

summary Presenta un breve resumen sobre el estado de DNA. Este es el valor por omisión.

Ejemplo: show executor

```
Node Volatile Summary
Executor node      = 2,26 (gato)
State              = on
Identification     = DECnet-MC68360 V1 R2.0 NP00523 [P10]
```

Ejemplo: show executor characteristics

Este ejemplo muestra la configuración completa de la base de datos del direccionador. El mandato **list executor characteristics** presenta, básicamente, la misma pantalla.

```
Node Volatile Characteristics
Executor node      = 2,26 (gato)
State              = on
Identification     = DECnet-MC68360 V1 R2.0 NP00523 [P10]
Physical address   = AA-00-04-00-1A-08
Type               = DEC-area
Routing version    = V2.0.0
Broadcast routing timer = 180
Maximum address    = 64
Maximum cost       = 1022
Maximum hops       = 30
Maximum visits     = 63
Maximum area       = 63
Max broadcast nonrouters = 64
Max broadcast routers = 32
Area maximum cost  = 1022
Area maximum hops  = 30
Maximum buffers    = 103
Buffer size        = 2038
```

Ejemplo: list executor status

Este ejemplo muestra el estado del direccionador en la base de datos permanente:

```
Node Permanent Status = 2,26 (gato)
Executor node         = on
State                 = DEC-area
Type
```

Ejemplo: **show executor counters**

Este ejemplo muestra los contadores que lleva DNA.

```
Node Volatile Counters = 2,26 (gato)
Executor node         = 525948
525948 Seconds since last zeroed
0 Aged packet loss
0 Node unreachable packet loss
0 Node out-of-range packet loss
0 Oversized packet loss
0 Packet format error
0 Partial routing update loss
0 Verification reject
```

Los elementos siguientes definen los campos que se muestran cuando usa el mandato **show/list executor**.

area maximum cost

Costo máximo permitido a un área.

area maximum hops

Número máximo de saltos permitidos a un área.

broadcast routing timer

Frecuencia de envío de mensajes de direccionamiento en caso de que no haya ningún cambio.

buffer size

Tamaño del almacenamiento intermedio para el direccionador.

executor node

Dirección del nodo y nombre del nodo. El nombre del nodo es el nombre establecido por el mandato **set hostname** de CONFIG.

identification

Identificación del software del direccionador, tal como la envían los mensajes de ID del sistema MOP.

maximum area

Área más alta para la que se mantienen rutas.

maximum broadcast nonrouters

Número máximo de nodos finales que pueden ser adyacentes de este direccionador.

maximum broadcast routers

Número máximo de direccionadores que pueden ser adyacentes de este direccionador.

maximum buffers

Número máximo de almacenamientos intermedios de paquetes del direccionador.

maximum cost

Costo máximo permitido a un nodo.

maximum hops

Número máximo de saltos permitidos a un nodo.

maximum visits

Número máximo de direccionadores por los que un paquete puede direccionarse entre origen y destino.

physical address

Dirección de Ethernet física establecida en todos los circuitos de Ethernet cuando se inicia DNA. Se deriva del ID de nodo.

routing version

La versión siempre es Versión 2.0.0.

state El estado de DNA, on (activado) u off (desactivado).

type ROUTING IV o AREA, que corresponden a nivel 1 y nivel 2.

module access-control circuit-specifier *argumento*

Establece una lista de las listas de control de acceso de DECnet que se han definido en la base de datos permanente para el direccionador, así como los contadores de su uso. Las opciones para los especificadores de circuitos son las siguientes:

all circuits

Especifica todos los circuitos del direccionador.

circuit [nombre]

Especifica el circuito nombrado.

known circuits

Especifica todos los circuitos del direccionador.

Los elementos siguientes son los argumentos que puede seleccionar después de entrar el mandato **show/list module access-control** y el especificador de circuito:

counters Indica los contadores de uso de las listas de control de acceso.

status Muestra información detallada sobre las listas de control de acceso, incluyendo los filtros de las mencionadas listas.

summary Muestra información resumida sobre el estado de las listas de control de acceso. Este es el valor por omisión.

Ejemplo: `show module access-control circuit eth/0 counters`

Ejemplo: `list module access-control circuit eth/0 counters`

```
Module Access-Control Volatile Counters
Circuit = Eth/0
6337      Seconds since last zeroed
0         Packets processed
0         Packets rejected
0         Access control loop iterations
```

module routing-filter circuit-specifier *argumento*

Establece una lista de los filtros de direccionamiento de áreas de DECnet que se han definido en la base de datos permanente para el direccionador.

all circuits

Especifica todos los circuitos del direccionador.

circuit [nombre]

Especifica el circuito nombrado.

known circuits

Especifica todos los circuitos del direccionador.

Los elementos siguientes son los argumentos que puede seleccionar después de entrar el mandato **show/list module routing-filter** y el especificador de circuito:

status Muestra información detallada sobre los filtros de direccionamiento, incluyendo la lista de áreas.

summary Muestra información de resumen sobre el estado de los filtros de direccionamiento. Este es el valor por omisión.

Ejemplo: `show module routing-filter circuit eth/0 status`

Ejemplo: `list module routing-filter circuit eth/0 status`

Zero

Use el mandato **zero** para borrar los contadores del circuito de la base de datos volátil, los contadores globales de dicha base de datos y los contadores del módulo de listas de control de acceso.

Sintaxis:

```
zero          circuit-specifier  
                executor  
                module access-control circuit-specifier
```

circuit-specifier

all circuits

Especifica todos los circuitos del direccionador.

circuit [nombre]

Especifica el circuito nombrado.

known circuits

Especifica todos los circuitos del direccionador.

Ejemplo: `zero all circuits`

executor Establece todos los contadores globales de la base de datos volátil en cero. No hay opciones.

Ejemplo: `zero executor`

module access-control circuit-specifier

all circuits

Especifica todos los circuitos del direccionador.

circuit [nombre]

Especifica el circuito nombrado.

Ejemplo: `zero module access-control all circuits`

Uso de OSI/DECnet V

Este capítulo describe la implementación del direccionador de la International Standards Organization's (ISO) Open Systems Interconnection (OSI) Connectionless Network Layer. DECnet Phase V soporta a OSI (de ahora en adelante llamado DECnet V/OSI) y los usuarios de redes DNA V pueden consultar este capítulo para obtener información sobre los protocolos ISO OSI. Este capítulo contiene las secciones siguientes:

- "Visión general de OSI"
- "Direccionamiento de NSAP" en la página 368
- "Direcciones de difusión múltiple" en la página 370
- "Direccionamiento OSI" en la página 371
- "Protocolo IS-IS" en la página 371
- "Protocolo ESIS" en la página 381
- "Circuitos X.25 para DECnet V/OSI" en la página 382
- "Configuración de OSI/DECnet V" en la página 384
- "Acceso al entorno de configuración de OSI" en la página 387
- "Mandatos de configuración de OSI/DECnet V" en la página 387

Visión general de OSI

Una red OSI está formada por varias subredes interconectadas. Una subred consiste en sistemas principales conectados a los que se denomina sistemas finales (ES) y direccionadores denominados sistemas intermedios (IS), tal como se muestra en la Figura 19.

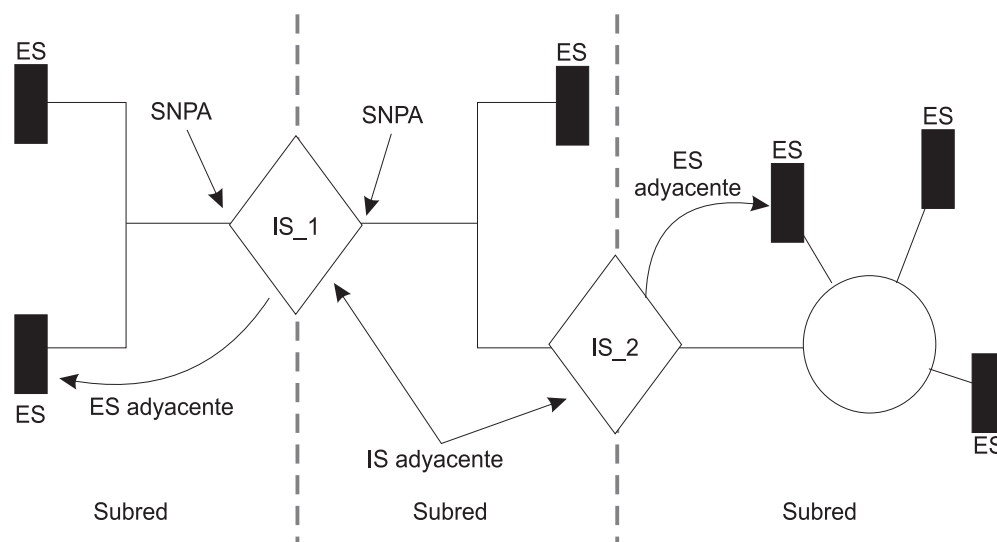


Figura 19. Red OSI

Los ES contienen todas las capas del modelo de referencia OSI y las aplicaciones del sistema principal. Los IS ejecutan las funciones de las tres capas inferiores del modelo de referencia OSI y manejan el direccionamiento de las unidades de datos del protocolo de red (NPDU) entre las subredes. Los IS se conectan lógicamente a la subred en el punto de conexión de ésta (SNPA). El SNPA es el punto de acceso a la capa de enlace de datos.

Según la configuración del IS, cada IS puede ejecutar tres protocolos: ES-IS, IS-IS y Connectionless-Mode Network Protocol (Protocolo de red en modalidad sin conexión - CLNP).

El protocolo ES-IS habilita a los ES e IS conectados a la misma subred para que descubran dinámicamente su respectiva existencia. Un ES conectado a la misma subred que un IS es adyacente de éste. El protocolo de direccionamiento IS-IS habilita a los IS para:

- Descubrir dinámicamente la existencia y disponibilidad de los IS adyacentes.
- Intercambiar información de direccionamiento con otros IS.
- Usar la información de direccionamiento intercambiada para calcular rutas basadas en el recorrido más corto.

El protocolo CLNP es un protocolo de datagramas que transporta paquetes entre IS.

Direccionamiento de NSAP

El NPDU contiene direcciones de red de OSI (también llamadas NSAP). El NSAP se refiere a un punto de la capa de la red donde el usuario accede a dicha capa. Los NSAP son puntos únicos dentro de un sistema que representan puntos finales direccionables de comunicación a través de la capa de red. El número de NSAP puede variar de sistema a sistema.

Una autoridad de direccionamientos como, por ejemplo, el National Institute of Standards and Technology (NIST) del gobierno de los Estados Unidos, administra las direcciones NSAP y determina cómo se asignan e interpretan las direcciones dentro del dominio. Si es necesario, estas autoridades pueden dividir el dominio en subdominios y designar las autoridades correspondientes para administrarlos.

Dentro del NPDU hay dos direcciones NSAP, una dirección de destino y una dirección de origen. La longitud de cada dirección puede variar entre 2 y 20 octetos y, por lo general, se representa en notación hexadecimal. A continuación, se muestra un ejemplo de un NSAP de 6 octetos que puede entrarse en la configuración OSI del direccionador.

AA000400080C

Dado que la longitud de la dirección es variable, las partes de la cabecera del PDU llamadas indicador de longitud de la dirección de destino e indicador de longitud de la dirección de origen, se usan para indicar la longitud, en octetos, de cada dirección.

Una dirección NSAP está formada por dos partes: una parte de dominio inicial (IDP) y una parte específica de dominio (DSP) tal como se muestra en Figura 20.



Figura 20. Estructura de dirección de NSAP

IDP

La IDP está formada por dos partes, el Authority and Format Identifier (Identificador de formato y autoridad - AFI) y el Initial Domain Identifier (Identificador de dominio inicial - IDI).

El AFI especifica el tipo de IDI y la autoridad de direccionamiento de red responsable de asignar los valores al IDI.

El IDI especifica el dominio de direccionamiento de red del que se asignan los valores de la DSP y la autoridad de direccionamiento de red responsable de asignar valores de la DSP de dicho dominio.

DSP

La autoridad de direccionamiento de la red identificada por el IDI determina la DSP. No obstante, es importante que la DSP incluya información de direccionamiento específica para el dominio.

Formato de direccionamiento IS-IS

El protocolo IS-IS divide la dirección NSAP en tres partes: dirección de área, ID del sistema y selector (consulte la Figura 21). La dirección de área y el ID del sistema junto con un selector con un valor de 0 se denominan Network Entity Title (Título de la entidad de red - NET). NET es la dirección de la capa de red en sí y se asigna cuando se configura un IS en la red OSI.

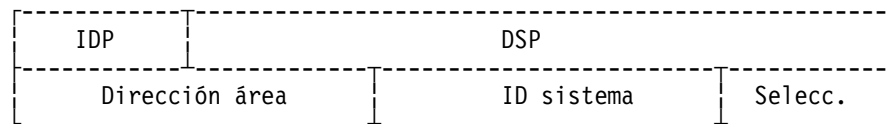


Figura 21. Interpretación de direccionamiento NSAP IS-IS

Dirección de área

En el protocolo IS-IS, la dirección de área es la parte de la NSAP que incluye toda o una parte de la IDP y la parte de la DSP hasta el ID del sistema.

La dirección del área corresponde a la parte de la NSAP que identifica un área específica de un dominio. Esta dirección debe tener, como mínimo, una longitud de 1 octeto y todos los ES e IS de la misma área deben tener la misma dirección de área.

ID del sistema

ID del sistema que corresponde a la parte de la NSAP que identifica un sistema específico de un área. Los ID de sistema deben tener los atributos siguientes:

- De 1 a 8 octetos de longitud.
- La misma longitud en todo el dominio. Los direccionadores usan una longitud de configuración por omisión de 6 octetos.
- Deben ser únicos para cada sistema en todo el dominio.

Selector

El selector es un campo de 1 octeto que actúa como selector para la entidad que va a recibir la PDU, por ejemplo, la capa de transporte o la misma capa de red IS. El direccionador establece este campo en 0.

NSAP de GOSIP Versión 2

Government Open Systems Interconnection Profile (GOSIP) Versión 2 proporciona, para el uso del gobierno, el formato de direccionamiento ilustrado en la Figura 22. Las autoridades responsables de las direcciones han definido claramente los campos y especificado el formato de direccionamiento bajo la DSP establecido por el National Institute of Standards and Technology (NIST).

IDP			DSP					
AFI	IDI	Ver	Aut.	Reserv.	Dominio	Área	ID. sis	Selecc.
47	0005	80			(2)	(2)	(6)	(1)

Figura 22. Formato de dirección GOSIP

- AFI** Este campo de 1 octeto tiene una designación (hexadecimal) de 47. Este valor significa que la dirección está basada en el formato ICD y que la DSP utiliza una sintaxis binaria.
- IDI** Este campo de 2 octetos tienen una designación (hexadecimal) de 0005. Este valor está asignado al gobierno de los E.E.U.U. y el NIST ha establecido el formato.
- VER** Este campo de 1 octeto tiene una designación de 80 (hexadecimal). Este valor identifica el formato de la DSP.
- Auth. (Authority)** Este campo de 3 octetos identifica la autoridad que controla la distribución de las direcciones NSAP.
- Reserved** Este campo de 2 octetos se proporciona para acomodar un crecimiento futuro.
- Domain** Este campo de 2 octetos contiene el identificador de dominios de direccionamiento.
- Area** Este campo de 2 octetos contiene el ID de área.
- Sys. ID** Este campo de 6 octetos identifica el sistema.
- Selector** Este campo de 1 octeto selecciona la entidad que recibirá la NPDU.

Direcciones de difusión múltiple

El direccionamiento de difusión múltiple es el método que los IS de nivel 1 (L1) y nivel 2 (L2) usan para distribuir actualizaciones de estado de enlace (LSU) y mensajes hello a otros sistemas o redes LAN. Cuando una LSU o un mensaje hello es de difusión múltiple, un grupo de estaciones de destino recibe el paquete. Por ejemplo, una LSU L1 es de difusión múltiple únicamente con otros IS L1. Un Intermediate System Hello (Hello de sistema intermedio - ISH) es de difusión múltiple únicamente con los ES de la misma subred.

Puede configurar direcciones de difusión múltiple para cada subred con el mandato **set subnet**. La Tabla 106 en la página 371 establece una lista de las direcciones de difusión múltiple de las LAN Ethernet y de red en anillo.

Tabla 106. Direcciones de difusión múltiple IS-IS

Destino	Ethernet 802.3	Red en Anillo 802.5	Descripción de la dirección
Todos los ES	09002B000004	C00000004000	Para todos los sistemas finales de la subred.
Todos los IS	09002B000005	C00000008000	Para todos los sistemas intermedios de la subred.
Todos los IS L2	0180C2000015	C00000008000	Para todos los sistemas intermedios L2 de la subred.
Todos los IS L1	0180C2000014	C00000008000	Para todos los sistemas intermedios L1 de la subred.

Direccionamiento OSI

OSI direcciona paquetes con el protocolo IS-IS. El direccionamiento con este protocolo se basa en:

- Un ID de sistema para direccionar dentro de un área
- Una dirección de área para direccionar dentro de un dominio
- El prefijo de dirección accesible para el direccionamiento para fuera del dominio

El protocolo IS-IS utiliza tablas de direccionamiento para reenviar los paquetes a los destinos correctos. Las entradas de dichas tablas se crean a partir de la información contenida en la base de datos de estado de los enlaces o de las direcciones accesibles configuradas por el usuario. La base de datos de estado de los enlaces se crea a partir de la información recibida en la actualización del estado del enlace (LSU). Consulte "Bases de datos de estados de enlaces" en la página 376.

Protocolo IS-IS

El protocolo IS-IS es un protocolo de direccionamiento dinámico del estado de los enlaces que detecta y aprende las mejores rutas a los destinos accesibles. IS-IS puede percibir rápidamente los cambios en la topología de un dominio y, después de un corto período de convergencia, calcular rutas nuevas. Para ello, el IS usa los paquetes siguientes:

- Link State Updates (Actualizaciones del estado de los enlaces - LSU) que el IS usa para mantener actualizada la información de la base de datos de estado de los enlaces.
- Sequence Number PDU (PDU del número de secuencia - SNP) para mantener la base de datos sincronizada y para asegurarse de que cada IS adyacente sabe cuál fue el Link State Packet (paquete de estado del enlace - LSP) más reciente de cada direccionador.
- Mensajes hello que los IS usan para descubrir, inicializar y mantener adyacencias con IS vecinos.

Áreas IS-IS

Un área IS-IS es un conjunto de sistemas en subredes continuas. La topología de cada área queda oculta de las de otras áreas para reducir el tráfico de direccionamiento. Se usa un IS de nivel 1 (L1) para direccionar dentro de un área. Los IS de nivel 2 (L2) se usan para direccionar entre áreas o sobre el troncal. Un IS que encamine dentro de un área o sobre el troncal se considera un IS L1/L2.

Dominio IS-IS

Un dominio IS-IS es un conjunto de normas, administradas por la misma autoridad, que deben seguir todos los ES e IS para asegurar la compatibilidad. Existen dos tipos de dominio que requieren discusión, dominio administrativo y dominio de direccionamiento.

Dominio administrativo

Un dominio administrativo controla la organización de los IS en dominios de direccionamiento así como las direcciones de subred o NSAP que usan dichos dominios de direccionamiento.

Dominio de direccionamiento

Un dominio de direccionamiento es un conjunto de IS y ES gobernados por las normas siguientes:

- Todos los dispositivos usan el mismo tipo de métrica de direccionamiento.
- Todos los dispositivos usan el mismo protocolo de direccionamiento como, por ejemplo, IS-IS.

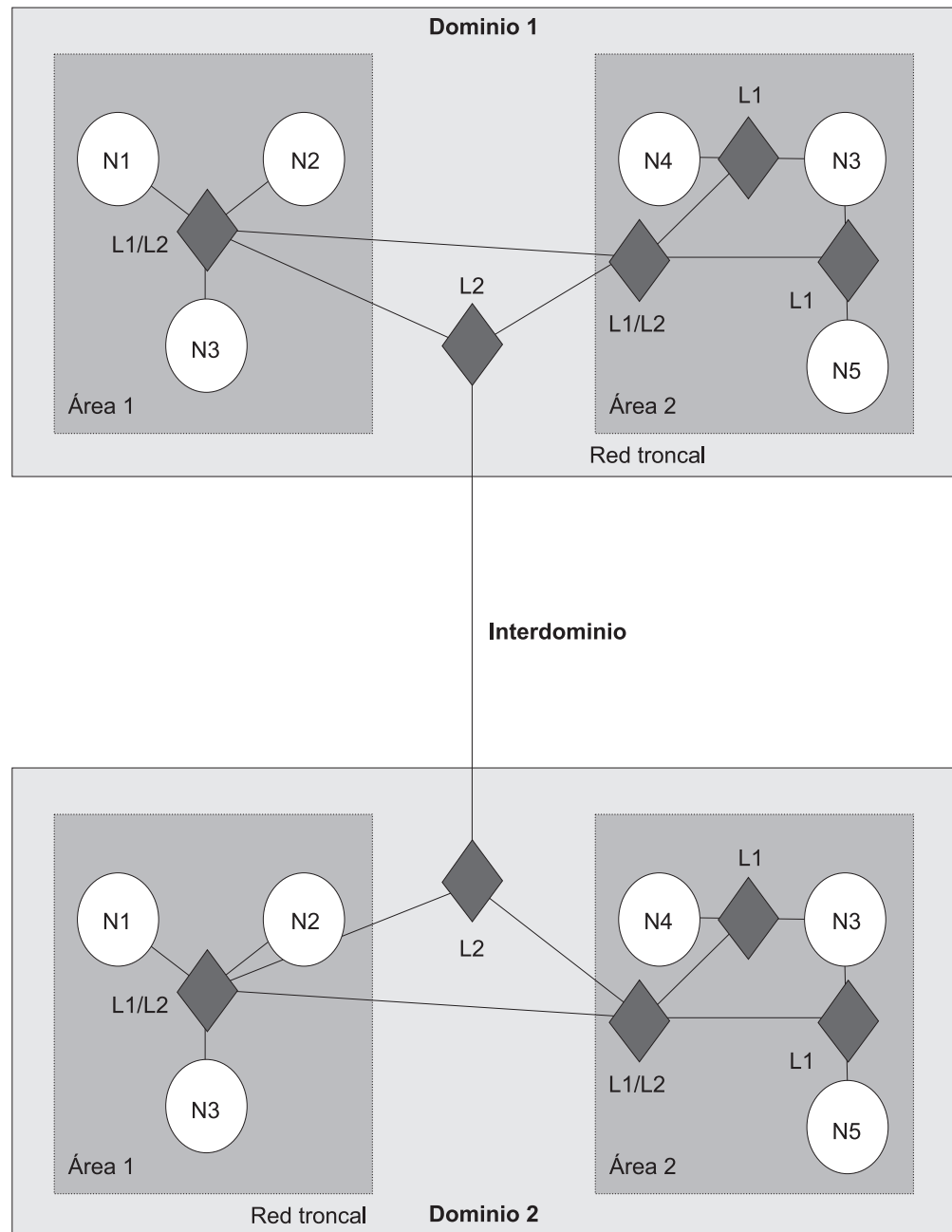


Figura 23. Dominio OSI

Áreas sinónimas

Cuando un IS L1 da servicio a más de un área, las áreas adicionales reciben el nombre de áreas sinónimas. Un direccionador puede dar soporte a cualquier cantidad de dichas áreas, siempre y cuando haya una solapación, como mínimo, de una dirección de área entre direccionadores adyacentes. Por ejemplo, en la Figura 24 en la página 374, el área 1 y el área 2 son sinónimas entre sí y las áreas 3 y 4 también son sinónimas entre sí.

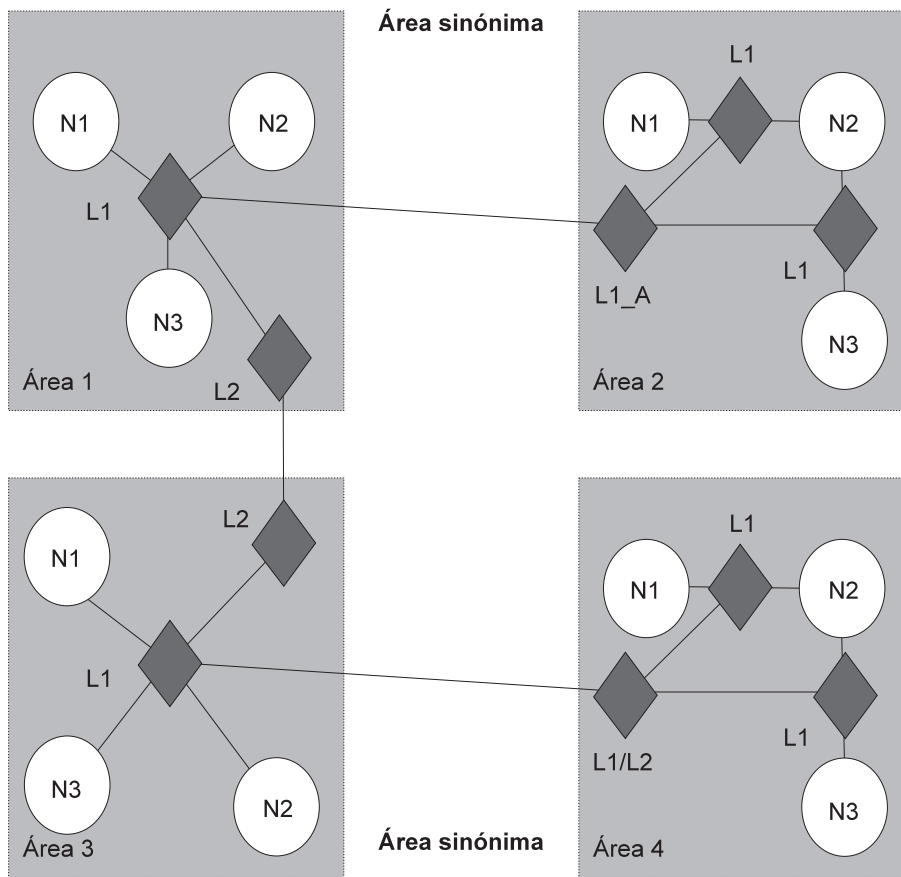


Figura 24. Áreas sinónimas

El L1_A IS del área 2 debe tener la dirección del área 1 añadida en su configuración y el IS L1 del área 1 debe tener la dirección del área 2 añadida en su configuración. Para que las áreas 3 y 4 sean sinónimas, debe añadirse la dirección de cada área a los otros IS L1.

Mensaje hello de IS a IS (IIH)

El mensaje IIH habilita a un IS para que determine la existencia de otros IS y para establecer adyacencias. Existen tres tipos de mensajes IIH: L1, L2 y punto a punto.

Cada IS contiene un temporizador hello local y un temporizador de retención. Cada vez que el temporizador hello expira, se ejecuta un difusión múltiple de un IIH sobre la interfaz del IS a cualquier IS adyacente. Cuando se recibe el mensaje hello, el destinatario establece o actualiza (renueva) la información de adyacencia. Esta información seguirá siendo actual durante el período de tiempo (en segundos) especificado por el temporizador de retención. Si el temporizador de retención se agota, se desactivará la adyacencia.

Mensaje L1 IIH

El mensaje L1 IIH se ejecuta en difusión múltiple sobre la interfaz cuando el temporizador hello local se agota. El IS L1 pone la información siguiente en el IIH:

- ID de origen
- Cualquier dirección de área manual a la que preste servicio
- Tipo de IS (sólo L1 o L1/L2)

- Prioridad
- ID de la LAN
- Si es aplicable, el ID de sistema del IS designado L1 (pseudonodo)

Al recibir este mensaje, el IS L1 adyacente extrae el ID de origen del IS emisor. A continuación, construye su propio mensaje IIH y pone su ID de origen en el campo de ID de origen. El ID de origen del remitente se pone en el campo de IS vecinos. La devolución del ID del remitente sirve a éste de verificación para saber que el IS adyacente es consciente de que existe (adyacencia en 2 sentidos).

Cuando el primer IS recibe el IIH, también extrae el ID de origen y mira en el campo de IS vecino. Al descubrir su propio ID de origen en el campo de IS vecino, este IS establecerá una adyacencia con el otro IS.

Nota: Antes de que el IS L1 adyacente pueda aceptar el paquete, éste deberá tener una dirección de área común y la misma longitud de ID del sistema que el IS adyacente.

Mensaje L2 IIH

El L2 IIH se ejecuta en difusión múltiple sobre sus interfaces con el fin de identificarse ante otros IS L2. El IS L2 tiene la misma función que un L1 IIH. El IS L2 pone la información siguiente en el IIH:

- ID de origen
- Cualquier dirección de área manual a la que preste servicio
- Tipo de IS (sólo L2 o L1/L2)
- Prioridad
- ID de la LAN
- Si es aplicable, el ID del sistema del IS designado L2.

Nota: Antes de que el IS L2 pueda aceptar el paquete, éste deberá tener la misma longitud de ID del sistema que el IS adyacente.

Mensaje IIH de punto a punto

Un mensaje IIH de punto a punto se envía sobre una interfaz de no difusión de IS (Frame Relay o X.25) para identificarse ante otros IS. Este IS da el IIH que contiene la información siguiente:

- ID de origen
- Cualquier dirección de área manual a la que preste servicio
- Tipo de IS (sólo L1, sólo L2 o L1/L2)
- ID del circuito local

IS designado

El IS designado se selecciona entre todos los IS conectados a la misma LAN para ejecutar funciones adicionales. En concreto, genera actualizaciones de estado de enlaces en nombre de la LAN y trata a ésta como si fuera un pseudonodo. Un pseudonodo es un método de modelación de toda la LAN como si fuera un nodo en la red con menos enlaces lógicos. La minimización de los enlaces lógicos en todo el dominio disminuye la complejidad de cálculo del algoritmo del estado del enlace.

Cuando una LAN tiene más de un IS, cada IS compara lo indicado a continuación para determinar qué IS se convertirá en el IS designado:

- Todos los IS comparan sus prioridades. Aquel que tenga la mayor prioridad se convertirá en el IS designado.
- Si los IS tienen la misma prioridad, compararán sus direcciones MAC de origen. Aquel que tenga la dirección de MAC numéricamente mayor se convertirá en el IS designado para la LAN y se indicará mediante el ID LAN.

Bases de datos de estados de enlaces

Cada IS L1 e IS L2 contiene una base de datos de estados de enlaces. El elemento primario de la base de datos es la actualización del estado del enlace (LSU). El direccionador es responsable de crear su propia LSU y de procesar las de otros IS para mantener la base de datos. La base de datos de L1 contiene información sobre ES. Cada base de datos de L1 es idéntica para todos los IS L1 de la misma área. La base de datos de L2 contiene información sobre áreas y direcciones accesibles. Cada base de datos de L2 es idéntica a la de todos los IS L2 configurados en el dominio IS-IS. Gracias a la información obtenida de las bases de datos, el algoritmo de direccionamiento Dijkstra calcula las vías de acceso más cortas a todos los destinos y crea las tablas de direccionamiento.

Inundación del estado de enlace

Para asegurarse de que cada IS L1 y IS L2 mantiene una base de datos idéntica, se inunda toda un área o un troncal con LSU. La inundación es un mecanismo utilizado por un IS L1 o IS L2 para propagar una LSU a todos los IS L1 o IS L2. Un IS L1 sólo inunda con LSU los IS L1. Un IS L2 sólo inunda con LSU los IS L2. Un IS L1/L2 acepta LSU de L1 y L2.

Actualización del estado del enlace de L1 (no pseudonodo)

Todos los IS L1 se inundan con la L1 LSU. El IS L1 da a la LSU la información siguiente:

- ID de origen
- Cualquier dirección de área manual a la que preste servicio
- Tipo de IS (L1)
- ID del sistema y costos de acceder a las adyacencias de IS
- Si es aplicable, los pseudonodos adyacentes del ID de sistema
- Los ID de sistema de cualquier adyacencia ES manual

Actualización del estado del enlace de L1 (pseudonodo)

Todos los IS L1 del área se inundan con la LSU del pseudonodo L1. Cualquier IS L1 situado en la misma LAN que reciba la LSU propagará dicha LSU a todos los IS L1 adyacentes del resto de sus subredes. El IS L1 pone la información siguiente en la LSU:

- ID de origen
- Tipo de IS (L1)
- ID de sistema y costo de acceder a todos los IS que no son pseudonodos situados en la LAN
- Los ID de sistema de cualquier adyacencia ES aprendida mediante un protocolo ES-IS

Actualización del estado de enlace L2 (no pseudonodo)

Todos los IS L2 se inundan con la L2 LSU. La IS L2 pone la información siguiente en su LSU:

- ID de origen
- Conjunto de direcciones de área a las que da servicio
- Tipo de IS (L2)
- ID de sistema y costo de acceder a las adyacencias de IS
- Si es aplicable, el ID de sistema del pseudonodo
- Prefijos de dirección para los IS situados en un dominio externo

Actualización del estado de enlace L2 (pseudonodo)

La LSU del pseudonodo L2 se ejecuta en difusión múltiple sobre la interfaz y se propaga a todos los IS L2 situados fuera de la subred. Cualquier IS no pseudonodo L2 situado en la misma subred que reciba la LSU pasará ésta en relé a todos los L2 situados fuera de la subred. La IS L2 pone la información siguiente en la LSU:

- ID de origen
- Tipo de IS (L2)
- ID de sistema y métricas de los IS no pseudonodos situados en la misma subred

IS L2 conectados y sin conectar

Un IS L2 conectado es un direccionador que tiene conocimiento de otras áreas. Un IS L2 sin conectar es un direccionador que no sabe que existen otras áreas aparte de él mismo.

Al direccionar, un IS L2 desconectado direcciona paquetes al IS L2 conectado más cercano.

Tablas de direccionamiento

Un IS sólo L1 usa una tabla de direccionamiento, la tabla de direccionamiento de nivel 1. Un IS sólo L2 contiene tres tablas de direccionamiento: una tabla de direccionamiento de direcciones de áreas L2, una tabla de direccionamientos de prefijos de direcciones accesibles métrica e internamente y una tabla de direccionamientos de prefijos de direcciones accesibles métrica y externamente. Un IS L1/L2 contiene la tabla de direccionamientos L1 y todas las tablas de direccionamiento L2. Las entradas de la tabla de direccionamientos se crean a partir de la información de la base de datos de estados de enlaces.

Direccionamiento de L1

A continuación, resumimos el direccionamiento de L1:

1. Un IS L1 recibe un paquete y compara la parte correspondiente a la dirección del área de la dirección de destino situada en la cabecera del paquete, con el conjunto de direcciones de áreas del direccionador.
2. Si el paquete está destinado al área del direccionador, éste extraerá el ID del sistema de la dirección. Al buscar una coincidencia, el direccionador comparará el ID del sistema con los ID de sistemas de la tabla de direccionamientos de L1.
3. Si encuentra una coincidencia, el IS direccionará el paquete al ES o al IS del salto siguiente. Si no encuentra ninguna coincidencia, eliminará el paquete.

4. Si el paquete no está destinado a dicha área, L1 reenviará el paquete al IS L2 más cercano o si el direccionador es un IS L1/L2, comprobará las tablas de direccionamiento de L2, tal como describimos en la sección siguiente. Si el L1 no puede determinar a dónde direccionar el paquete, éste se eliminará.

Direccionamiento de L2

Un IS L2 contiene tres tablas de direccionamiento: una tabla de direccionamientos de direcciones de áreas L2, una tabla de prefijos de direcciones accesibles métrica e internamente (interna) y una tabla de prefijos de direcciones accesibles métrica y externamente (externa).

A continuación, resumimos el direccionamiento de L2:

1. Un IS L2 recibe un paquete y compara la parte correspondiente a la dirección de destino de la cabecera con el conjunto de direcciones de áreas de la tabla de direccionamientos de direcciones de áreas. Si encuentra una coincidencia, el paquete se reenviará al direccionador troncal del salto siguiente. Si no encuentra ninguna coincidencia, el direccionador comprobará la tabla de direccionamientos interna.
2. La tabla de direccionamientos interna contiene entradas de prefijos de direcciones accesibles que llevan a otros dominios. Si la tabla de direccionamientos interna contiene una coincidencia, se reenviará el paquete por el troncal al dominio adecuado. Si no se encuentra ninguna coincidencia, el direccionador comprobará la tabla de direccionamientos externa.
3. La tabla de direccionamientos externa contiene entradas de prefijos de direcciones accesibles que también llevan a otros dominios. Si la tabla de direccionamientos externa contiene una coincidencia, se reenviará el paquete por la vía de acceso al dominio adecuado. Si no encuentra ninguna coincidencia, eliminará el paquete.

Consulte “Direccionamiento externo e interno” en la página 379 para obtener una explicación detallada sobre las tablas de direccionamiento internas y externas.

Métrica de direccionamiento

Una métrica de direccionamiento es un valor asociado a una función del circuito para indicar el costo del direccionamiento sobre dicho circuito. Por ejemplo, la métrica de direccionamiento basada en el gasto monetario de un circuito usará un valor bajo para indicar que el gasto monetario es bajo y un valor alto para indicar que el gasto monetario del direccionamiento de un paquete sobre dicho circuito es elevado.

El protocolo de direccionamiento IS-IS usa cuatro métricas de direccionamiento: la métrica por omisión, la métrica de retardo, la métrica de gastos y la métrica de errores.

La implementación actual del modelo OSI usa únicamente la métrica por omisión IS-IS. Por convenio, la métrica por omisión, tiene por objetivo medir la capacidad del circuito para manejar el tráfico. Todos los IS del dominio de direccionamientos deben ser capaces de calcular rutas basadas en la métrica por omisión. El resto de las métricas de direccionamiento son opcionales. Aunque esta implementación del protocolo OSI no las usa, las describimos a continuación por motivos meramente informativos.

- La métrica de retardo mide el retardo de tránsito del circuito asociado.

- La métrica de gastos mide el costo monetario de utilizar el circuito asociado.
- La métrica de errores mide la probabilidad de que se produzcan errores residuales en el circuito asociado.

Direccionamiento externo e interno

Un direccionamiento externo o interno implica que un IS L2 direcciona un paquete entre dos dominios separados. Cuando es necesario direccionar un paquete a otro dominio, el IS L2 intenta que la dirección coincida con un prefijo de dirección accesible de la tabla de direccionamientos externa o interna. Las rutas externas e internas se basan en el costo (métrica de direccionamiento) de llegar al destino. El costo de una ruta interna tiene en cuenta el costo del direccionamiento dentro del dominio y el de direccionamiento al destino. El costo de una ruta externa se basa únicamente en el costo del direccionamiento al destino fuera del dominio de direccionamiento. El IS elige la vía de acceso con el costo más bajo.

Por ejemplo, si un paquete está destinado a ir del nodo A del dominio 1 al nodo D del dominio 2 (Figura 25 en la página 380). El nodo A puede elegir entre dos vías de acceso para enviar el paquete: al nodo B y después al nodo D o bien al nodo C y después al nodo D. La forma en que los nodos B y C anuncien el costo de sus rutas a D determinará cómo el nodo A decidirá direccionar el paquete, ya sea interna o externamente. Existen tres opciones posibles:

- Los nodos B y C anuncian el costo de sus rutas a D como interno. El costo interno de la ruta A-B-D es 35, que es el costo de direccionar de A a B, más el de direccionar de B a D. El costo interno de la ruta A-C-D es 40, que es el costo de direccionar de A a C, más el de direccionar de C a D. En este caso, el nodo A elegirá direccionar sobre la vía de acceso A-B-D ya que el costo es inferior.
- Los nodos B y C anuncian el costo de sus rutas como externo. El costo externo de A-B-D es 30, que es el costo de direccionar de B a D. El costo externo de A-C-D es 20. En este caso, el nodo A elegirá direccionar sobre la vía de acceso A-C-D porque el costo de esta ruta es inferior.
- Los nodos B y C anuncian el costo de sus rutas como interno y externo. El costo interno y externo de las rutas se añade a sus tablas de direccionamiento respectivas. Dado que se prefieren las rutas internas a las externas, el direccionador elegirá la ruta interna A-B-D.

Nota: Dado que no existe un protocolo de direccionamiento externo, todas las rutas de prefijo entre dominios deben configurarse estáticamente.

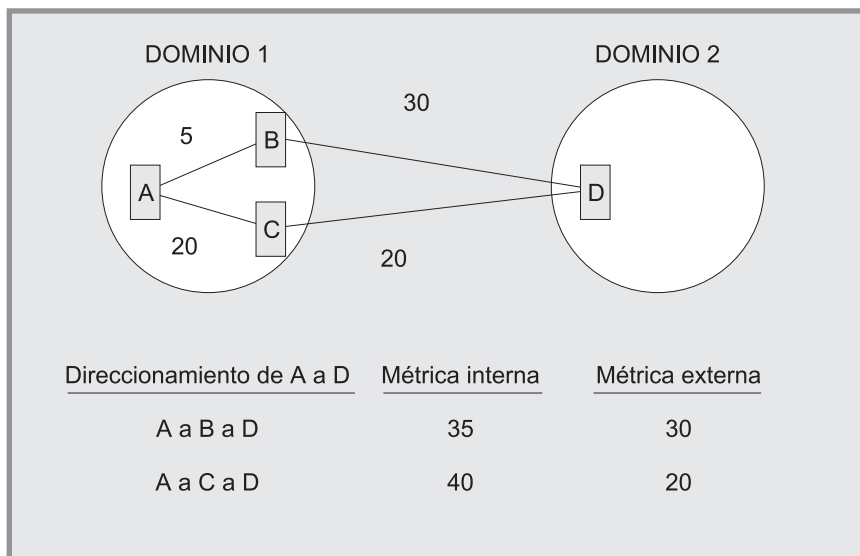


Figura 25. Métricas de direccionamiento externo e interno

Codificación de prefijos de direcciones

Cuando entre rutas de prefijos de direcciones, tenga muy en cuenta la diferencia existente entre las normas de codificación para NSAP y para rutas de prefijos. Los cuatro ejemplos siguientes ilustran la codificación de prefijos de direcciones.

Codificación de un IDI de longitud fija

Para varios prefijos de direcciones, codificar el prefijo y el NSAP correspondiente es lo mismo. Por ejemplo, si está usando la dirección GOSIP 1.0 y desea crear una ruta a una organización de DoD. El IDI de Org es 1234 y el IDI de DoD es 0006. La dirección de NSAP codificada será

4700061234CCCC222222222222

El prefijo de la dirección codificada es el resultado de truncar el NSAP

4700061234

Las normas de codificación tratan todos los formatos de NSAP que tengan un IDI de longitud fija y todos los prefijos de dirección que acaban después del IDP.

Codificación de un AFI

Un prefijo de dirección basado completamente en el AFI sólo se codifica en el campo AFI de 1 octeto. Por ejemplo, si necesita un prefijo de dirección para todas las direcciones de formato X.121 (usadas en redes X.25), usará un AFI de X.121 que tenga un valor de 37.

Codificación de un IDI de longitud variable

Las direcciones de NSAP que tienen formatos de IDI de longitud variable como, por ejemplo, X.121, F.69, E.163 y E.164, usan un esquema de codificación más complicado. Cuando los IDI de longitud variable se codifican como un NSAP, la dirección se rellena a la izquierda con ceros; no obstante, cuando se codifica el IDI como un prefijo de dirección, no se rellena en la izquierda.

Por ejemplo, desea que la ruta X.25 llame desde los E.E.U.U. a una portadora X.25 situada en los Países Bajos. Supongamos que la portadora tiene un Data Network Identifier Code (Código identificador de la red de datos - NDIC) 2041. La codificación del prefijo de la dirección será

372041

Un abonado a X.25 que tenga un número de teléfono nacional (NTN) de 117010 en esta portadora tendrá un NSAP de

3700002041117010

Observe que el IDI del NSAP se rellena a la izquierda con ceros hasta alcanzar los 14 dígitos ya que el número de datos internacionales resultantes (2041117010) era inferior a 14 dígitos.

No obstante, si desea un prefijo de dirección que apunte únicamente a un abonado de X.25, la codificación será el NSAP (3700002041117010), ya que el prefijo no acaba en el IDP.

Prefijos de dirección por omisión

El prefijo de dirección por omisión se usa cuando desea originar una ruta por omisión a todas las direcciones situadas fuera del dominio. Los prefijos de dirección por omisión tienen una longitud de cero, por lo que no hay que codificar nada.

Contraseñas de autenticación

Para proporcionar una capa mínima de seguridad a la red, OSI tiene una opción de contraseñas de autenticación. Cuando ésta se habilita, el IS no aceptará ningún paquete IS-IS que no contenga la contraseña adecuada. El campo de autenticación de la NPDU contiene las contraseñas de autenticación. Existen dos tipos de estas contraseñas: de transmisión y de recepción.

Se añade una contraseña de transmisión a los paquetes IS-IS que transmite el IS. Una contraseña de recepción es un listado de contraseñas de transmisión que el IS acepta. Por ejemplo, con la autenticación habilitada, si no se añade una contraseña de transmisión al paquete, o no hay un listado de contraseñas de transmisión en la base de datos de contraseñas de recepción, se eliminará el paquete. Existen tres tipos de contraseñas de recepción y transmisión: de dominio, de área y de circuito.

Una contraseña de dominio proporciona seguridad a la información de direccionamiento de L2. Una contraseña de área proporciona seguridad a la información de direccionamiento de L1. Una contraseña de circuito proporciona seguridad a los mensajes hello de IS-IS.

Protocolo ESIS

El protocolo ES-IS habilita a los ES e IS conectados a la misma subred para que descubran dinámicamente su respectiva existencia y disponibilidad. Esta información también permite a los ES obtener información de todos ellos sin que haya un IS disponible.

La información de redirección de ruta habilita a un IS para que informe a un ES de la existencia de una ruta mejor al reenviar NPDU a un destino en concreto. Por

ejemplo, una ruta mejor puede ser otro IS situado en la misma subred que el ES o el ES de destino situado en la misma subred.

Mensaje hello

La información de direccionamiento se pasa a los ES e IS mediante mensajes hello.

Cada ES y cada IS tienen un temporizador de configuración local (CT) y un temporizador de retención (HT). Cada vez que el CT se agota, se envía en difusión múltiple un mensaje hello a la LAN. Cuando este mensaje se recibe, el destinatario establece el valor del HT de acuerdo con el valor transmitido en el campo HT del mensaje. Se espera que el destinatario retenga esta información hasta que el HT se agote, para asegurar el funcionamiento correcto del protocolo ES-IS.

Mensaje hello de sistema final (ESH)

El mensaje ESH se envía en difusión múltiple desde el ES a todos los IS L1 cuando el CT local se agota. El ES crea este mensaje para informar a un IS sobre cualquier NSAP al que dé servicio. Al recibir el mensaje, el IS extrae la información SNPA y NSAP y almacena el par en la tabla de direccionamientos L1, sustituyendo cualquier otra información que estuviera almacenada.

Mensajes hello de sistema intermedio (ISH)

El mensaje ISH se envía en difusión múltiple a todos los ES adyacentes cuando el CT local se agota. El IS crea este mensaje para informar al ES de su NET. Al recibir el mensaje, el ES extrae la información SNPA y NET y almacena el par en una de las tablas de direccionamiento locales, sustituyendo cualquier otra información que estuviera almacenada.

Circuitos X.25 para DECnet V/OSI

En el caso de las redes X.25, el direccionador establece circuitos virtuales conmutados (SVC) X.25 en los circuitos de direccionamiento.

Nota: Para habilitar DECnet V/OSI para X.25, debe entrar en el proceso de DECnet IV y definir el direccionador para que sea un direccionador DEC-AREA o DEC-ROUTING-IV. Debe ejecutar esta operación (y reiniciar el direccionador) para habilitar los mandatos para la configuración de DECnet V/OSI. Use el mandato **define executor type**.

Circuitos de direccionamiento

Los circuitos de direccionamiento son conexiones de punto a punto entre nodos que implementan el protocolo ISO CLNS. El direccionador emplea los circuitos de direccionamiento siguientes:

- Circuitos de entrada estáticos
- Circuitos de salida estáticos
- Circuitos asignados dinámicamente

Los circuitos de entrada y de salida estáticos sólo tienen un SVC asociado a ellos y llevan tanto datos del usuario como datos que no son del usuario (como mensajes de protocolo de direccionamiento). Los circuitos estáticos se activan y desactivan explícitamente usando mandatos de configuración DECnet V/OSI. Los

circuitos de direccionamiento asignados dinámicamente se establecen al llegar los datos y se borran cuando no se reciben ni se transmiten datos. Un circuito asignado dinámicamente puede tener varios SVC, pero sólo puede transportar datos del usuario.

DECnet V/OSI controla las llamadas de cada uno de los tipos de circuitos de direccionamiento usando *filtros* y *plantillas*. Los filtros se usan para procesar las llamadas de entrada, mientras que las plantillas se usan para establecer las llamadas de salida.

Filtros

Un *filtro* es un conjunto de parámetros que el usuario puede configurar y que definen los criterios para aceptar las llamadas de entrada destinadas al circuito de direccionamiento X.25 especificado.

Los parámetros definidos en un filtro incluyen la dirección DTE de llamada, una prioridad de filtro y los datos del usuario/llamada.

Filtros y circuitos de direccionamiento

Las llamadas de entrada pueden estar en un circuito de entrada estático o en un circuito asignado dinámicamente (DA). Puede definir uno o varios filtros en el mismo circuito de direccionamiento. Por ejemplo, un circuito DA puede tener varias adyacencias y puede definirse más de un filtro para él.

Prioridades del filtro

Las lista de filtros de los circuitos de entrada estáticos y de los circuitos DA se entremezclan y la mezcla está ordenada por prioridad descendente. Cuando se recibe una llamada de entrada, el direccionador busca primero la mayor prioridad en la lista de filtros. Para evitar que se asigne erróneamente un circuito estático a un circuito DA, se recomienda asignar a los filtros de todos los circuitos estáticos una prioridad superior a la de los filtros de todos los circuitos DA.

Restricciones de los filtros a las llamadas

En el caso de un circuito de entrada estático, el filtro debe especificar una dirección DTE de llamada concreta, pero el primer octeto de los datos de llamada/usuario debe contener el discriminador de protocolos ISO 8473 (129). Para que varios circuitos DA funcionen correctamente, deberán configurarse restricciones adicionales para cada filtro definido. Esto asegurará que los criterios de selección especificados en dichos filtros permitan efectuar la distinción necesaria entre las llamadas de entrada.

Nota: Si un circuito DA se conecta incorrectamente con un circuito estático, la arquitectura no intentará identificar la condición o rectificar el problema. En el lado estático se generará el “fallo de inicialización” usual debido a una falta de respuesta a las consultas de inicialización de enlaces. Por consiguiente, el SVC estático se borrará posteriormente.

Plantillas

Una plantilla es un conjunto de parámetros que el usuario puede configurar para las llamadas de salida. La plantilla establece los parámetros para que el circuito del direccionador remoto acepte las llamadas de entrada. Los parámetros definidos en una plantilla incluyen la dirección DTE de llamada y los datos del usuario/llamada.

Sólo puede definir una plantilla por circuito de direccionamiento estático de salida.

Inicialización de enlaces

La inicialización de enlaces es un procedimiento propiedad de Digital Equipment Corporation (y no forma parte de OSI). Esta inicialización se efectúa inmediatamente después del establecimiento del SVC. Se usa principalmente para establecer la relación de DECnet con un sistema remoto en un enlace de punto a punto.

Al recibir un mensaje de inicialización/XID, puede efectuarse la verificación en dos niveles: basándose en el circuito o bien en el sistema. Básicamente, el proceso de verificación compara los datos de verificación de entrada con datos especificados localmente para el circuito o para el sistema de llamada. Los datos de verificación aparecen en el campo de datos de verificación del mensaje XID.

Nota: Este release del software de direccionador no da soporte a la verificación efectuada por el sistema.

Configuración de OSI/DECnet V

Nota: Cuando trabaje con redes DNA IV mezcladas con redes DNA V, deberá efectuar toda la supervisión y configuración de DNA IV desde el proceso de configuración de DNA IV NCP>. Para obtener información sobre la configuración de DNA IV, Consulte "Uso de DNA IV" en la página 327. El uso de "OSI" en este capítulo se refiere a los entornos OSI y DNA V a menos que se indique lo contrario.

Procedimiento de configuración básico

En esta sección se indican los pasos de configuración mínimos necesarios para activar y ejecutar el protocolo OSI/DNA V sobre una LAN (Ethernet o red en anillo), redes de conmutación de paquetes X.25 y Frame Relay. Antes de empezar cualquier procedimiento de configuración, use el mandato **list device** del proceso **config** para establecer una lista de los números de interfaz de los diferentes dispositivos. Si desea obtener más información sobre los mandatos de configuración, consulte los mandatos de configuración descritos en el presente capítulo.

Nota: Para que los cambios de configuración nuevos entren en vigor, deberá reiniciar el direccionador.

Siga el procedimiento de configuración básico siguiente antes de empezar los procedimientos especializados descritos en las secciones siguientes.

Establecimiento del título de la entidad de red (NET)

Establezca el NET del direccionador usando el mandato **set network-entity-title**. El NET está formado por el ID de sistema del direccionador y su dirección de área. Use el mandato **list globals** para verificar que NET esté configurado correctamente.

Habilitación global de OSI

Habilite el software de OSI para que se ejecute en el direccionador usando el mandato **enable OSI**. Use el mandato **list globals** para verificar que el protocolo OSI esté habilitado.

Configuración de OSI sobre una LAN Ethernet o red en anillo

Para configurar el protocolo OSI para que se ejecute sobre una LAN Ethernet o red en anillo, establezca la subred. Existe una correspondencia de una a una entre las subredes y las interfaces. Use el mandato **set subnet** para configurar todas las subredes LAN (Ethernet y red en anillo). Use las direcciones de difusión múltiple por omisión para Ethernet. Cuando configure una red en anillo, use las direcciones siguientes:

Parámetro	Dirección funcional 802.5
All ESs (Todos los ES) [09002B000004]	C00000004000
All ISs (Todos los IS) [09002B000005]	C00000008000
All L1 ISs (Todos los IS L1) [0180C2000014]	C00000008000
All L2 ISs (Todos los IS L2) [0180C2000015]	C00000008000

Use el mandato **list subnet detailed** o **list subnet summary** para verificar que haya configurado correctamente las subredes.

Configuración de OSI sobre X.25 o Frame Relay

Para configurar el protocolo OSI para que se ejecute sobre la interfaz de X.25 o Frame Relay, haga lo siguiente:

Establezca la subred Use el mandato **set subnet** para establecer la interfaz en X.25 o FRL (Frame Relay). Use los valores por omisión para toda la información necesaria. Use el mandato **list subnet detailed** o **list subnet summary** para verificar que haya configurado correctamente las subredes.

Establezca el circuito virtual Use el mandato **set virtual-circuit** para configurar un circuito virtual X.25 o Frame Relay.

Nota: El direccionador le solicitará una dirección DTE. Para frame relay, entre el número de DLCI (Data Link Control Identifier - Identificador del control del enlace de datos). Para X.25 entre la dirección DTE de PSN.

Configuración de un direccionador DNA V para un entorno DNA IV

Cuando configure un direccionador DNA V, es posible que deba configurar una interfaz para ejecutar un entorno DNA IV. Por ejemplo, el direccionador se conecta a una red DNA V y DNA IV, o un ES de DNA IV está conectado a un direccionador de DNA V.

Antes de empezar a seguir los pasos que indicamos a continuación, use la sección anterior adecuada para configurar OSI sobre una LAN, X.25 o Frame Relay.

1. Entre en el proceso de configuración de DN. Salga de `OSI config>` y entre `NCP>`. Use el mandato **protocol DN**.
2. Defina la dirección DNA global. Use el mandato **define executor address** para configurar el nodo DNA y el número de área del direccionador.
3. Habilite globalmente DNA. Use el mandato **define executor state** para habilitar el protocolo DNA para que se ejecute en el direccionador.
4. Habilite el direccionamiento entre áreas. Si el algoritmo de direccionamiento L2 es el vector de distancia del nivel 2, use el mandato **define executor type**

area para asegurarse de que este direccionador pueda intercambiar información de direccionamiento de nivel 2 de DNA IV.

5. Habilite el circuito DNA IV. Habilite el circuito que usará el direccionador para intercambiar la información de direccionamiento. Use el mandato **define circuit type state on**.

Consideraciones de algoritmo de DNA IV y DNA V

DNA IV usa un algoritmo de direccionamiento de vector-distancia. DNA V puede usar un algoritmo de direccionamiento de vector-distancia o de estado-enlace. El algoritmo se selecciona de acuerdo con lo que está habilitado o inhabilitado y las combinaciones que pueden producirse con estos dos protocolos.

DNA IV inhabilitado y OSI/DNA V habilitado

Se considera que esta combinación es un entorno OSI/DNA V puro y se establece el algoritmo automáticamente en estado-enlace en los niveles 1 y 2 sin tener en cuenta cómo está configurado el mandato **set algorithm**.

DNA IV habilitado y OSI/DNA V inhabilitado

Se considera que esta combinación es un entorno DNA IV puro y se establece el algoritmo automáticamente en vector-distancia sin tener en cuenta cómo está configurado el mandato **set algorithm**.

DNA IV habilitado y OSI/DNA V habilitado

Se trata de un entorno mezclado y se lee y configura la información del algoritmo a partir de la SRAM. Use el mandato **set algorithm** para configurar esta información en la SRAM.

Configuración y supervisión de OSI/DECnet V

Este capítulo describe los mandatos de supervisión y configuración de OSI/DECnet V e incluye las secciones siguientes:

- “Acceso al entorno de supervisión de OSI/DECnet V” en la página 415
- “Mandatos de supervisión de OSI/DECnet V” en la página 415

Acceso al entorno de configuración de OSI

Para obtener información sobre cómo acceder al entorno de configuración de OSI, consulte “Getting Started (Introduction to the User Interface)” en el manual *Guía del usuario de software*.

Mandatos de configuración de OSI/DECnet V

Esta sección resume y después explica los mandatos de configuración de OSI. Estos mandatos le permiten crear o modificar una configuración de OSI. Entre todos los mandatos de configuración de OSI después del indicador `OSI Config>`. Los valores por omisión de los mandatos y sus parámetros se ponen entre corchetes inmediatamente después del indicador.

Los mandatos de configuración manipulan la base de datos de OSI permanente (SRAM).

Tabla 107 (Página 1 de 2). Resumen de mandatos de configuración de OSI

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte la sección “Cómo obtener ayuda” en la página xxix.
Add	Añade áreas a las que da soporte este nodo; recibe contraseñas con objetivos de autenticación; pone prefijos a direccionadores para otros dominios y alias
Change	Modifica algunos parámetros establecidos con el mandato add .
Clear	Borra una contraseña recibida, una contraseña de transmisión o una SRAM
Delete	Suprime áreas, PVC, direcciones-prefijo, adyacencias, alias, subredes y parámetros del circuito de direccionamiento X.25.
Disable	Inhabilita una subred, el protocolo OSI o un circuito de direccionamiento X.25.
Enable	Habilita una subred, el protocolo OSI o un circuito de direccionamiento X.25.
List	Muestra la configuración actual de las adyacencias, alias, contraseñas, pvc, direcciones-prefijo, subredes, algoritmo, phaseivpfx, información global o circuitos de direccionamiento X.25.

Tabla 107 (Página 2 de 2). Resumen de mandatos de configuración de OSI	
Mandato	Función
Set	Configura las propiedades asociadas a parámetros OSI (conmutadores, valores globales, NET, temporizadores, subredes, contraseñas-transmisión, direcciones-prefijo, adyacencias, pvc, algoritmos y phaseivpfx)
Exit	Le devuelve al nivel de mandatos anterior. Consulte la sección "Cómo salir de un entorno de nivel inferior" en la página xxix.

Add

Use el mandato **add** para configurar direcciones de prefijo y área, recibir contraseñas y dar alias a direcciones.

Sintaxis:

```

add          alias
              area...
              filter...
              prefix-address
              receive-password
              routing-circuit...
              template...
    
```

alias Añade una serie de caracteres ASCII que designa una dirección de área o un ID de sistema en particular. Esta serie puede utilizar caracteres incluidos entre *a-z*, *A-Z*, *0-9*, otros caracteres entre los que se incluye el guión (-), la coma (,) y el subrayado (_). No use caracteres de escape.

El desplazamiento indica la posición, en semioctetos (porciones), donde la serie de caracteres empieza dentro de la dirección (alias usados para ID del sistema que tienen un desplazamiento de 1). Esta serie debe tener el mismo tamaño o longitud que el segmento al que designa o recibirá un mensaje indicando *invalid segment length* (longitud de segmento no válida). El alias máximo permitido es de 20 bytes.

Nota: Cuando use una entrada de alias, deberá ponerla entre corchetes. Por ejemplo: **I1_update**
47[nombrenuevo]99999000012341234.

Ejemplo:

```

add alias
Alias [ ]:
Segment [ ]:
Offset [1]:
    
```

Alias La serie de caracteres que desea utilizar

Segment El segmento NSAP al que sustituirá el alias.

Offset La situación del alias (en 4 bits, semioctetos) dentro del NSAP. El desplazamiento se determina desde el principio (izquierda) del NSAP tal como aparece en el terminal.

area *dir-área*

Añade direcciones de área adicionales (máximo de 18 bytes) a las que da soporte el nodo. Un nodo L1 que da soporte a otras áreas considera a éstas sinónimas. Una dirección de área es la parte del área del NET configurado. Si intenta añadir una dirección de área duplicada, el direccionador mostrará un mensaje de error.

Ejemplo:

```
add area 47000580999999000012341234
```

Nota: Cuando añada áreas sinónimas a un nodo L1, use el mandato **set globals** para configurar el número máximo de áreas sinónimas permitidas para este nodo. Todos los direccionadores de un área deben usar el número máximo de áreas sinónimas. No pueden establecerse adyacencias si son diferentes.

filter *nombre-filtro nombre-circuito-direccionamientos DTE-llamada Datos prioridad usuario llamada*

Añade parámetros en los que el direccionador basa su aceptación de las llamadas X.25 de entrada en un circuito de direccionamientos, ya sea un circuito de entrada estático o un circuito asignado dinámicamente (DA).

El *nombre-filtro* es el nombre que da al filtro. El *nombre-circuito-direccionamiento* es el nombre del circuito de direccionamiento con el que está asociado el filtro.

El *DTE-llamada* es la dirección del direccionador que llama.

El direccionador local comprueba la dirección del DTE de una llamada de entrada con una lista de filtros con prioridades para todos los circuitos. Una *prioridad* de filtro superior en la lista significa que primero se establece una conexión con la dirección del DTE de llamada del filtro. Se recomienda que asigne una mayor prioridad a los filtros para los circuitos estáticos que para los circuitos DA. Esto puede evitar que una llamada estática de entrada se asigne a un circuito DA.

El valor *Datos usuario llamada* puede ser uno de los tres valores siguientes: *osi*, *dec* o *user*.

- En el caso de *osi*, el direccionador configura automáticamente un discriminador de protocolos ISO para los datos de la llamada y ésta debe ser una llamada de un nodo OSI.
- En el caso de *dec*, el direccionador espera que las llamadas de entrada sean de un direccionador Digital Equipment Company (Compañía de equipos digitales).
- En el caso de *user*, se le solicitará una entrada adicional con un máximo de 16 octetos. Entre texto para restringir la aceptación de las llamadas de entrada. El campo *Datos usuario llamada* de la llamada de entrada debe coincidir con el texto especificado.

Ejemplo:

```
add filter
Filter Name [ ]:
Routing Circuit Name [ ]:
DTE Address [ ]:
Call UserData (OSI/DEC/USER):
```

Mandatos de configuración de OSI/DECnet V (Talk 6)

Si selecciona **user** aparecerá un indicador adicional para que entre datos del usuario, seguido de un indicador de prioridad:

```
(max 16 octets) [ ]?  
Priority (1-10) [5]?
```

prefix-address

Añade rutas estáticas a destinos situados fuera del dominio IS-IS. Este parámetro le solicita información diferente según el tipo de subred (X.25, LAN o FRL) que se configuró usando el mandato **set subnet**.

Nota: Si no se entra ningún prefijo de dirección, se asumirá el prefijo por omisión.

Ejemplo:

Subred LAN:

```
add prefix-address  
Interface Number [0]:  
Address Prefix [ ]:  
MAC Address [ ]:  
Default Metric [20]:  
Metric Type [Internal]:  
State [ON]:
```

Subred X.25:

```
add prefix-address  
Interface Number [0]:  
Address Prefix [ ]:  
Mapping Type[Manual]:  
DTE Address[]:  
Default Metric[20]:  
Metric Type [Internal]:  
State [ON]:
```

Subred Frame Relay:

```
add prefix-address  
Interface Number [0]:  
Address Prefix [ ]:  
DTE Address [ ]:  
Default Metric [20]:  
Metric Type [Internal]:  
State [ON]:
```

Nota: Si la subred no existe, recibirá el mensaje de error Subnet does not exist - cannot define a reachable address (La subred no existe - no se puede definir una dirección accesible).

Interface Number

Define la interfaz sobre la que se accede a la dirección

Address Prefix

Define el prefijo de NSAP (máximo de 20 bytes).

MAC Address

Define la dirección del MAC de destino. Debe especificar esta dirección si la interfaz corresponde a una subred LAN. Este indicador sólo aparecerá si la interfaz está conectada a una subred LAN.

Mapping Type

Define cómo se determina la dirección física de destino, manual o X.121.

Mandatos de configuración de OSI/DECnet V (Talk 6)

Si es manual, el protocolo le solicitará la dirección del DTE.

Si es X.121, el protocolo no le solicitará la dirección del DTE. En este caso, esta dirección se extraerá del NSAP.

DTE Address

Define la dirección del DTE de destino. Debe especificar esta dirección si la interfaz es X.25 y el tipo de correlación es manual. Este indicador sólo aparece si se configura la interfaz para X.25 y el tipo de correlación es manual.

Default Metric

Define el costo de la dirección.

Metric Type

Define si el costo métrico se usa para el direccionamiento externo (E) o interno (I).

State

Cuando se establece en ON (activo), esta dirección-prefijo se anuncia a otros direccionadores de L2. Cuando se establece en OFF (inactivo), se trata de una dirección-prefijo no funcional.

routing-circuit

Añade un canal de comunicaciones para los circuitos virtuales conmutados X.25 (SVC) que la capa de direccionamiento usa para enviar y recibir datos.

El parámetro del circuito de direccionamiento sólo se puede aplicar si configura el direccionador como direccionador de tipo DEC. Puede especificar uno de los tipos de circuito de direccionamiento siguientes:

- estático entrada
- estático salida
- asignado dinámicamente

Un circuito estático de entrada maneja las llamadas X.25 de entrada. Un filtro de llamadas (consulte **add filter**) especifica los datos que usará el direccionador para aceptar o rechazar llamadas de entrada al circuito. Un circuito de salida estático inicia las llamadas X.25 de salida. El direccionador usa una plantilla de llamadas (consulte **add template**) para efectuar llamadas de salida. Un circuito asignado dinámicamente puede tener varios SVC que se ejecuten simultáneamente. A diferencia de los circuitos estáticos, el direccionador usa un circuito asignado dinámicamente únicamente cuando hay tráfico de entrada o salida del direccionador. Cierra el circuito asignado dinámicamente al agotarse el temporizador de desocupación.

El mandato **add routing-circuit** le solicita los valores de sus parámetros.

Ejemplo:

```
add routing-circuit
Interface number [0]?
Circuit Name [ ]?
Circuit Type (STATIC/DA) [STATIC]?
Circuit Direction (OUT/IN) [OUT]?
```

Si selecciona **STATIC** y **OUT**, aparecerán los indicadores adicionales siguientes:

Mandatos de configuración de OSI/DECnet V (Talk 6)

```
Recall Timer (0-65535) [60]?
Max Call Attempts (0-255) [10]?
Initial Min Timer (1-65535) [55]?
Enable IS-IS [YES]?
Level 2 only [NO]?
External Domain [NO]?
Default Metric [20]?
ISIS Hello Timer [3]?
Enable DECnetV Link Initialization [YES]?
Modify Receive Verifier (YES/NO) [NO]?
Transmit Verifier (YES/NO) [NO]?
Explicit Receive Verification (TRUE/FALSE) [TRUE]?
```

Si selecciona **STATIC** e **IN**, aparecerán los indicadores adicionales siguientes:

```
Initial Min Timer (1-65535) [55]?
Enable IS-IS [YES]?
Level 2 only [NO]?
External Domain [NO]?
Default Metric [20]?
ISIS Hello Timer [3]?
Enable DECnetV Link Initialization [YES]?
Modify Receive Verifier (YES/NO) [NO]?
Modify Transmit Verifier (YES/NO) [NO]?
Explicit Receive Verification (TRUE/FALSE) [TRUE]?
```

Si selecciona **DA** para el tipo de circuito, aparecerán los indicadores adicionales siguientes:

```
Recall Timer (0-65535) [60]?
Reserve Timer (1-65536) [600]?
Idle Timer (1-65536) [30]?
Max SVCs (1-65535) [1]?
```

Interface Number

Especifica la interfaz X.25 lógica de este circuito de direccionamiento.

Circuit Name

Establece el nombre alfanumérico de este registro de circuito de direccionamiento.

Circuit Type

Especifica si este circuito de direccionamiento es un circuito **STATIC** (estático) o **DYNAMICALLY ALLOCATED** (asignado dinámicamente).

Circuit Direction

Especifica **IN** (entrada) o **OUT** (salida) para determinar si el **SVC** del circuito estático se establecerá con una solicitud de llamada de entrada o una solicitud de llamada de salida. En ambos casos, se establece inicialmente el **SVC** sobre la acción del operador, pero el circuito no se habilita totalmente hasta que ambos extremos del circuito se hayan inicializado satisfactoriamente.

Recall Timer

Define el tiempo, en segundos, que debe esperar un circuito **DA** o un circuito estático de salida antes de intentar una solicitud de llamada nueva. Esto es el resultado del fallo de la solicitud de llamada inicial o de que una llamada posterior se haya borrado.

Max Call Attempts

Si falla una solicitud de llamada, Max Call Attempts define el número máximo de solicitudes de llamada posteriores que el circuito estático de salida intentará antes de abandonar. Llegado a este punto, el fallo de llamada se anotará cronológicamente y será necesaria la intervención del operador para activar el circuito estático de salida.

Initial Min Timer

Especifica el período de tiempo (en segundos) que esperará un circuito estático de salida para que se inicialice un enlace (recepción de un ESH o un ISH) después de que se haya aceptado la solicitud de llamada. Si el temporizador mínimo inicial se agota antes de que se haya inicializado completamente el enlace, el SVC se borrará y se generará un suceso que indicará un fallo de la inicialización.

Enable IS-IS

Define si el protocolo IS-IS está habilitado en este circuito de direccionamientos. Cuando se establece en ON, se habilita el protocolo IS-IS; cuando se establece en OFF, este protocolo no se habilita.

Level2 Only

Especifica si este circuito de direccionamientos se usa únicamente para direccionamientos de nivel 2.

External Domain

Especifica si el direccionador transmite y recibe mensajes a un dominio o desde un dominio situado fuera de su dominio de direccionamientos IS-IS.

Default Metric

Define el costo de esta dirección.

ISIS Hello Timer

Define el intervalo de tiempo transcurrido entre la transmisión de hellos ISIS.

Enable DECnetV Link Initialization

Define si la inicialización de enlaces de estilo DEC para este circuito está habilitada (YES) o no (NO).

Modify Receive Verifier

Especifica los datos de verificación que se comprobarán cuando se reciba un XID al verificar por circuito.

Modify Transmit Verifier

Especifica los datos de verificación que se incluirán en el XID.

Explicit Receive Verification

Define si la verificación se efectúa por circuito o por sistema. TRUE (VERDAD) especifica la verificación por circuito y FALSE (MENTIRA) especifica por sistema.

Reserve Timer

Define el tiempo transcurrido después de que el temporizador de desocupación se agote durante el cual el direccionador seguirá considerando un nodo remoto de un

circuito DA como "activo". El direccionador podrá reenviar datos en el circuito DA hasta que se agote el temporizador de reserva.

Idle Timer

Define el período de tiempo que puede estar desocupada una adyacencia DA (sin transmisión de datos) antes de borrarla.

Max SVCs

Define el número máximo de adyacencias SVC a las que este circuito DA da soporte. Si no puede efectuarse ninguna llamada debido a que se ha alcanzado el número máximo de adyacencias SVC, se generará un suceso "Exceed Max SVC adyacencias" (superado el número máximo de adyacencias SVC).

receive-password

Añade una serie de caracteres ASCII (hasta un máximo de 16 caracteres) que autentifica todos los paquetes de entrada. Un paquete de entrada cuya contraseña coincida con una de las contraseñas de recepción se procesará a través de IS; se eliminarán aquellos paquetes de entrada cuya contraseña no coincida.

Ejemplo:

```
add receive-password
```

Nota: Se obtendrá un mensaje de error si se usa un *tipo de contraseña* no válido.

```
Password type [Domain]:  
Password [ ]:  
Reenter password:
```

Password type

Designa uno de los dos tipos de contraseñas: *dominio* o *área*.

Las contraseñas de dominio se usan con LSP L2 (paquetes de estado del enlace, nivel 2) y SNP (PDU del número de secuencia).

Las contraseñas de área se usan con LSP L1 y SNP.

Password

Designa la serie de caracteres que se usa para la autenticación. La serie máxima que se permite tiene 16 caracteres.

template *nombre-plantilla nombre-circuito-direccionamiento DTE destino Datos usuario-llamada*

Crea una plantilla a través de la cual el direccionador efectúa llamadas de salida en un circuito de direccionamiento de salida estático. Las plantillas para circuitos de salida estáticos son análogas a los filtros para circuitos de entrada estáticos.

El *nombre-plantilla* es el nombre que da a la plantilla. El *nombre-circuito-direccionamiento* es el nombre del circuito de direccionamiento con el que está asociada la plantilla.

El *DTE-destino* es una dirección para el direccionador remoto que tiene un máximo de 14 dígitos.

Los *Datos usuario-llamada* deben coincidir con los datos de llamada establecidos en un filtro del circuito remoto. *Datos usuario-llamada* puede ser uno de los tres valores siguientes: *osi*, *dec* o *user*.

- En el caso de *osi*, el direccionador configura automáticamente un discriminador de protocolos ISO para los datos de la llamada y ésta debe ir a un direccionador ISO.
- En el caso de *dec*, los datos del usuario identifican las llamadas de salida como provenientes de un direccionador Digital Equipment Company.
- En el caso de *user*, se le solicitará una entrada adicional con un máximo de 16 octetos. Entre texto para que coincida con los datos de usuario del filtro adecuado en un direccionador remoto.

Ejemplo:

```
add template
  Template Name []?
  Routing Circuit Name []?
  DTE Address []?
  Call UserData (OSI/DEC/USER) ?
```

Si elige **user**, aparecerá este indicador adicional:

```
(max 16 octets) [] ?
```

Entre un máximo de 16 octetos de texto para los datos del usuario.

Change

Le permite modificar los parámetros de registros ISO/DNV creados en la base de datos permanente.

Sintaxis:

```
change          filter
                  prefix-address
                  routing-circuit
                  template
```

filter *nombre-filtro* Cambia los valores de los parámetros del filtro del circuito de direccionamiento. Puede entrar un nombre de filtro o dejar que el direccionador le solicite el nombre de filtro.

Los valores indicados entre corchetes [] son los valores actuales de los parámetros; el valor configurado que se lee en la base de datos permanente.

Ejemplo: change filter

```
Filter Name [currentvalue]?
DTE Address [currentvalue]?
Call Userdata (OSI/DEC/USER)? [currentvalue]?
```

Si selecciona **user**, aparecerá este indicador adicional para que entre datos del usuario, seguido de un indicador de prioridad:

```
(max 16 octets) [currentvalue] ?
```

prefix-address Cambia los datos de dirección para las subredes. El direccionador le solicitará los datos de dirección.

Ejemplo: change prefix-address

Subred LAN:

Interface Number [0]:
Address Prefix []:
MAC Address []:
Default Metric [20]:
Metric Type [Internal]:
State [ON]?

Subred X.25:

Interface Number [0]:
Address Prefix []:
Mapping Type [Manual]:
DTE Address []:
Default Metric [20]:
Metric Type [Internal]:
State [ON]?

Subred Frame Relay:

Interface Number [0]:
Address Prefix []:
DTE Address []:
Default Metric [20]:
Metric Type [Internal]:
State [ON]?

Interface Number

Indica la interfaz sobre la que se alcanza la dirección.

Address Prefix

Indica el prefijo del NSAP de destino (máximo de 20 bytes).

MAC Address

Indica la dirección del MAC de destino. Debe especificar esta dirección si la interfaz corresponde a una subred LAN. Este indicador sólo aparecerá si la interfaz está conectada a una subred LAN.

Mapping Type

Indica cómo se determina la dirección física de destino, *manual* o *X.121*.

Si es manual, el protocolo le solicitará la dirección del DTE.

Si es X.121, el protocolo no le solicitará la dirección del DTE. En este caso, esta dirección se extraerá del NSAP.

DTE Address

Define la dirección del DTE de destino. Debe especificar esta dirección si la interfaz es X.25 y el tipo de correlación es manual. Este indicador sólo aparece si se configura la interfaz para X.25 y el tipo de correlación es manual.

Default Metric

Indica el costo de la dirección.

Metric Type

Indica si el costo métrico se usa para el direccionamiento externo (E) o interno (I).

State

Cuando se establece en ON (activo), esta dirección recibirá paquetes. Cuando se establece en OFF (inactivo), se trata de una dirección no funcional.

routing-circuit nombrecircuitodireccionamiento Cambia los valores de configuración de un circuito de direccionamiento. Puede entrar un nombre de circuito de direccionamiento o dejar que el direccionador le solicite un

nombre. Los valores que están entre corchetes [] son los valores actuales que se leen en la base de datos permanente.

Ejemplo: change routing-circuit

```
Routing Circuit Name [currentvalue]?
Recall Timer (0-65535) [currentvalue]?
Max Call Attempts (0-255) [currentvalue]?
Initial Min Timer (1-65535) [currentvalue]?
Enable ES-IS [currentvalue]?
Enable IS-IS [currentvalue]?
Level 2 only [currentvalue]?
External Domain [currentvalue]?
Default Metric [currentvalue]?
ISIS IS Hello Timer [currentvalue]?
ISIS Hello Timer [currentvalue]?
Enable DECnetV Link Initialization [currentvalue]?
Modify Receive Verifier (YES/NO) [currentvalue]?
Modify Transmit Verifier (YES/NO) [currentvalue]?
Explicit Receive Verification (TRUE/FALSE) [currentvalue]?
```

template nombre-plantilla Cambia los valores de la plantilla de un circuito de direccionamiento de salida estático. Puede entrar un nombre de plantilla o dejar que el direccionador le solicite un nombre. Los valores indicados entre corchetes [] corresponden a los valores actuales de los parámetros; los valores configurados que se leen en la base de datos permanente.

Ejemplo: change template

```
Template Name [currentvalue]?
DTE Address [currentvalue]?
Call UserData (OSI/DEC/USER)? [currentvalue]
```

Si selecciona **user**, este indicador opcional aparecerá para que entre los datos de usuario; seguido de un indicador de prioridad:

```
(max 16 octets) [currentvalue] ?
Priority (1-10) [currentvalue]?
```

Clear

Use el mandato clear para borrar la SRAM o para eliminar la contraseña de transmisión o recepción.

Sintaxis:

```
clear           rceive-password
                sram
                transmit-password
```

receive-password

Elimina todas las contraseñas de recepción configuradas anteriormente usando el mandato **add receive-password**.

Nota: Si usa una contraseña no válida recibirá un mensaje de error.

Ejemplo: clear receive

```
Password Type [Domain]:
```

Password Type

Especifica el tipo de contraseña que se está usando:

Dominio o *Área*. Consulte el mandato

add receive-password para obtener una descripción de estas contraseñas.

SRAM

Use este parámetro para borrar la configuración OSI de la SRAM.

Atención: Use este mandato *únicamente* si tiene la intención de borrar la configuración.

Ejemplo:

```
clear sram
Warning: All OSI SRAM Information will be erased.
Do you want to continue? (Y/N) [N]?
```

Transmit-password

Elimina la contraseña de transmisión previamente configurada usando el mandato **set transmit-password**. El resultado de este parámetro es el mismo que el producido por el parámetro de la contraseña de recepción.

Nota: Si usa una contraseña no válida recibirá un mensaje de error.

Ejemplo:

```
clear password transmit
Password Type [Domain]:
```

Delete

Use el mandato **delete** para eliminar parámetros configurados previamente usando los mandatos **set** o **add**.

Sintaxis:

```
delete          adjacency
                  alias
                  area
                  filter (sólo configuración DEC)
                  prefix-address
                  routing-circuit
                  subnet
                  template (sólo configuración DEC)
                  virtual-circuit
```

adjacency

Elimina una adyacencia de ES configurada estáticamente con el mandato **set adjacency**.

Ejemplo:

```
delete adjacency
Interface Number [0]?
Area Address [ ]?
System ID [ ]?
```

Interface number

Indica la interfaz de la adyacencia.

Area address

Indica la dirección de área de la adyacencia.

System ID

Indica la parte del NET que identifica la adyacencia dentro del área.

alias Elimina la serie de caracteres ASCII que designa una parte de una dirección de área o un ID de sistema.

Ejemplo:

```
delete alias  
ALIAS [ ]?
```

area *dirección*

Elimina la dirección de área (*dirección*) configurada previamente con el mandato **add area**.

Ejemplo:

```
delete area 47000580999999000012341234
```

filter *nombre-filtro*

Elimina un registro de filtro de la base de datos permanente.

Ejemplo:

```
delete p_systems
```

prefix-address

Elimina la dirección-prefijo configurada previamente con el mandato **set prefix-address**.

Ejemplo: delete prefix-address

```
Interface Number [0]?  
Address Prefix [ ]
```

Interface number

Indica el número de interfaz sobre la que está configurada la dirección-prefijo.

Address Prefix

Indica el prefijo del NSAP de destino.

Interface number

Indica el número de la interfaz sobre la que está configurado el PVC.

DTE address

Indica la dirección del DTE de la red X.25 al que se está conectando o el DLCI de la red Frame Relay al que se está conectando.

routing-circuit *nombre-circuito-direccionamiento*

Elimina un circuito de direccionamiento X.25 que se estableció con **add routing-circuit** desde la base de datos permanente.

Ejemplo:

```
delete routing-circuit p_system2
```

subnet *núm.intfz*

Elimina una subred que se configuró previamente con el mandato **set subnet**. *núm.intfz* indica el número de interfaz de la subred configurada.

Ejemplo:

```
delete subnet 1
```

Mandatos de configuración de OSI/DECnet V (Talk 6)

template *nombre-plantilla*

Elimina la plantilla de un circuito de direccionamiento de salida estático mediante el cual el direccionador genera mensajes X.25 de salida a partir de la base de datos permanente.

Ejemplo:

```
delete template x25_5
```

virtual-circuit

Elimina un circuito virtual X.25 o Frame Relay que se configuró previamente con el mandato set virtual-circuit.

Ejemplo:

```
delete virtual-circuit  
Interface number [0]?  
DTE address []?
```

Interface number

Número de interfaz sobre el que está configurado el circuito virtual.

DTE address

Dirección del DTE de la red X.25 al que se está conectando o el DLCI de la red Frame Relay al que se está conectando.

Disable

Use el mandato **disable** para inhabilitar las funciones habilitadas previamente usando el mandato **enable**.

Sintaxis:

```
disable          osi  
                  routing-circuit  
                  subnet
```

osi Inhabilita el protocolo OSI en el direccionador.

routing-circuit *nombre-circuito-direccionamiento*

Inhabilita el circuito de direccionamiento especificado.

Use el mandato **add routing-circuit** para establecer circuitos de direccionamiento.

subnet *núm.interfaz*

Inhabilita el protocolo OSI en la subred especificada (*núm.interfaz*).

Ejemplo:

```
disable subnet 0
```

Enable

Use el mandato **enable** para habilitar el protocolo OSI o una subred OSI.

Sintaxis:

```
enable          osi  
                  routing-circuit...  
                  subnet...
```


osi Habilita el protocolo OSI en el direccionador.

routing-circuit *nombre-circuito-direccionamiento*

Habilita el circuito de direccionamiento especificado.

Use el mandato **add routing-circuit** para establecer circuitos de direccionamiento.

Ejemplo:

```
enable routing-circuit p_system2
```

subnet *núm.interfaz*

Habilita el protocolo OSI en la subred especificada (*núm.interfaz*).

Ejemplo:

```
enable subnet 0
```

List

Use el mandato list para visualizar la configuración actual del protocolo OSI.

Sintaxis:

```
list
    adjacencies
    algorithm
    alias
    filter (sólo configuración DEC)
    globals
    password
    phaseivpfx
    prefix-address
    routing-circuits (sólo configuración DEC)
    subnets
    templates (sólo configuración DEC)
    timers
    virtual-circuits
```

adjacencies

Muestra todas las adyacencias de ES configuradas estáticamente.

Ejemplo:

```
list adjacencies
Ifc   Area Address   System ID   MAC Address
0     0001-0203-0405  0001-0203-0405
1     0002-4000-0000  0000-0019-3004
```

Ifc Indica el número de la interfaz que se conecta con la adyacencia.

Area Address

Indica la dirección de área de esta adyacencia de ES.

System ID

Indica la parte del NET que identifica la adyacencia.

MAC Address

Indica la dirección de MAC (SNPA) de la adyacencia.

algorithm

Muestra el algoritmo de direccionamiento que está configurado en la SRAM para el protocolo DNA V. Si está ejecutando únicamente el protocolo OSI, este parámetro no tendrá soporte.

Ejemplo:

```
list algorithm
Level 1 algorithm LINK_STATE
Level 2 algorithm DISTANCE_VECTOR
```

Level 1 Algorithm

Indica la configuración actual del algoritmo de direccionamiento para nivel 1, estado del enlace (valor por omisión) o vector de distancia.

Level 2 Algorithm

Indica la configuración actual del algoritmo de direccionamiento para nivel 2, estado del enlace o vector de distancia (valor por omisión).

Nota: Según si DNA IV está habilitado o inhabilitado, el algoritmo de direccionamiento que se visualiza aquí será diferente de lo que se esté ejecutando en el direccionador.

alias Muestra los alias configurados y los segmentos de dirección correspondientes.

Ejemplo:

```
list aliases
Alias      Segment      Offset
joplin    AA0004000104      1
moon      0000931004F0      1
trane     000093E0107A      1
```

filter Muestra los filtros definidos para circuitos X.25.

Ejemplo:

```
list filters
Rout Cir Name  Filter Name  DTE Addr  Pri  Call Data
routeCir2     filter1      25        5    81
```

globals Muestra los parámetros globales de NET, direcciones de área, valores de conmutación y configuración del temporizador actuales del direccionador.

Ejemplo:

```
list globals
DNAV State: Enabled*  Network Entity Title: 4700050001:0000931004F0
Manual Area Addresses:
1. 4700050001  2. 7700050011

Switches:
ESIS Checksum = On           ESIS Init Option = Off
Authentication = Off

Globals:
IS Type = L2                 System ID Length = 6
L1 LSP Size = 1492 bytes    L2 LSP Size = 1492 bytes
Max IS Adjs = 50            Max ES Adjs = 200
Max Areas = 50              Max ESs per Area = 50
Max Ifc Prefix Adds = 100   Max Ext Prefix Adds = 100
Max Synonymous Areas = 3    Max Link State Updates = 100
```

OSI State or DNAV State

Indica si el protocolo OSI o el DNA V está ejecutándose en el direccionador.

Network Entity Title

Indica la dirección de área y el ID de sistema que forman el NET del direccionador.

Manual Area Addresses

Áreas en las que el direccionador funciona. La primera dirección de área refleja la dirección de área del NET configurado del direccionador. Las direcciones de área adicionales se añadieron con el mandato **add area**.

Globals: Indica los parámetros globales configurados actualmente:

IS Type

La designación del direccionador en el entorno OSI: L1 o L2.

Domain ID Length

El tamaño (en bytes) de la parte de ID del sistema de NET.

Nota: Todos los direccionadores del dominio deben estar de acuerdo en la longitud del ID del dominio.

L1 LSP Size/L2 LSP Size

Muestra el tamaño máximo del almacenamiento intermedio de LSP de L1 y L2.

Max IS Adjacencies/Max ES Adjacencies

Muestra el número máximo de adyacencias de IS y ES permitidas para todos los circuitos.

Max Areas

Muestra el número máximo de áreas del dominio de direccionamiento.

Max ESs per Area

Muestra el número máximo de ES permitidos en un área.

Max Int Prefix Adds

Muestra el número máximo de direcciones de prefijo interno.

Max Ext Prefix Adds

Muestra el número máximo de direcciones de prefijo externo.

Max Synonymous Areas

Muestra el número máximo de áreas de nivel 1 a las que da servicio este direccionador.

password

Muestra el número de las contraseñas de transmisión y recepción configuradas para cada dominio y área OSI. Las contraseñas de recepción se configuran con el mandato **add receive-password**. Las contraseñas de transmisión se configuran con el mandato **set transmit-password**.

Ejemplo:

Mandatos de configuración de OSI/DECnet V (Talk 6)

```
list password
Number of Passwords Configured:
  -- Domain --
Transmit = 3
Receive = 2
  -- Area --
Transmit = 4
Receive = 6
```

phaseivpfx

Muestra el prefijo de dirección de DNA phase IV configurado que está usando el protocolo OSI para direccionar paquetes a una red DNA IV conectada.

Ejemplo:

```
list phaseivpfx
Local Phase IV Prefix: 49
```

prefix-address

Muestra todas las SNPA de las rutas configuradas estáticamente.

Ejemplo:

```
list prefix:-addresses
Ifc Type Metric State Address Prefix Dest Phys Address
0 INT 20 On 470006 302198112233
1 EXT 50 OFF 470006 302198223344
```

Ifc Indica el número de la interfaz donde se puede acceder a la dirección.

Type Indica el tipo de métrica, interna (INT) o externa (EXT).

Metric Indica el costo de la dirección accesible.

Address prefix

Indica el prefijo del NSAP de destino. Este prefijo puede tener 20 bytes de longitud.

Dest Phys Address

Indica la dirección del DTE de destino si esta interfaz es X.25 y la correlación configurada es manual.

routing-circuits

Muestra un resumen de todos los circuitos de direccionamiento o detalles de cada circuito de direccionamiento.

Ejemplo:

Mandatos de configuración de OSI/DECnet V (Talk 6)

list routing circuits

Summary or Detailed [Summary]? Summary

Ifc	Name	Type	Enabled
0	routecir1	STATIC-OUT	YES
0	routecir2	STATIC-IN	YES
0	routecir3	DA	YES

Summary or Detailed [Summary]? Detailed

```
Routing Circuit Name [] routecir2
Interface #: 0
Enabled: YES
Type: STATIC
Direction: Incoming
Initial Minimum Timer: 55
Enable IS-IS: YES
L2 Only: NO
External Domain: NO
Metric: 20
IS-IS Hello Timer: 3
DECnetV Link Initialization: YES
Receive Verifier:
Transmit Verifier:
Explicit Receive Verification: TRUE
```

Interface # / Ifc

Especifica la interfaz X.25 lógica de este circuito de direccionamiento.

Name Establece el nombre alfanumérico de este registro de circuito de direccionamiento.

Enabled Indica el estado del circuito de direccionamiento: YES (Sí) para habilitado y NO para inhabilitado.

Type Indica si el circuito es STATIC-IN (ESTÁTICO DE ENTRADA), STATIC-OUT (ESTÁTICO DE SALIDA) o DA (asignado dinámicamente).

Direction Indica cómo establece el direccionador un circuito de direccionamiento estático: mediante una solicitud de llamada de entrada (IN) o una solicitud de llamada de salida (OUT).

En ambos casos, el SVC se establece inicialmente mediante una acción del operador, pero el circuito no se habilita completamente hasta que ambos extremos del circuito se hayan inicializado satisfactoriamente.

Initial Min Timer

Especifica el período de tiempo (en segundos) que esperará un circuito estático de salida para que se inicialice un enlace (recepción de un ESH o un ISH) después de que se haya aceptado la solicitud de llamada. Si el temporizador mín inicial se agota antes de que se haya inicializado completamente el enlace, el SVC se borrará y se generará un suceso que indicará un fallo de la inicialización.

Enable IS-IS

Indica si el protocolo IS-IS está habilitado en este circuito.

L2 Only Indica si este circuito de direccionamientos se usa únicamente para direccionamientos de nivel 2.

External Domain

Indica si el direccionador transmite y recibe mensajes a un dominio o desde un dominio situado fuera de su dominio de direccionamientos IS-IS.

Metric Especifica el costo de esta dirección.

Mandatos de configuración de OSI/DECnet V (Talk 6)

ISIS Hello Timer

Indica el intervalo de tiempo transcurrido entre la transmisión de hellos ISIS.

DECnetV Link Initialization

Indica si la inicialización de enlaces de estilo DEC para este circuito está habilitada (YES - Sí) o no (NO).

Receive Verifier

Muestra los datos de verificación que se comprobarán con un XID recibido al verificar por circuito.

Transmit Verifier

Muestra los datos de verificación que se incluirán en los XID cuando se verifique por circuito.

Explicit Receive Verification

Indica si la verificación la efectúa el circuito o el sistema. TRUE (VERDAD) indica verificación del circuito, FALSE (MENTIRA) indica verificación del sistema.

Subnet *inf.subred núm.intfz*

Muestra información de la subred.

- *Inf.subred* tiene dos opciones: Summary (resumida) o Detailed (detallada).
 - *Summary* muestra información de todas las subredes configuradas.
 - *Detailed* muestra únicamente información de las subredes LAN.
- *núm.Intfz* es la interfaz que se conecta con la subred.

Ejemplo:

```
list subnet summary
Ifc State Type  ISIS  ISIS  L2 Only  Ext Dom  Metric  EIH (sec)  IIH(sec)
0   On  LAN  Enb  Enb  False   False   20      10         3
2   On  X25
3   On  Fr1
```

Ifc Indica el número de interfaz de la subred.

State Indica el estado de la interfaz, ON (activo) u OFF (inactivo).

Type Indica el tipo de subred: LAN, X25,

ISIS Indica el estado del protocolo ES-IS, habilitado (Enb) o inhabilitado (Dis).

ISIS Indica el estado del protocolo IS-IS, habilitado (Enb) o inhabilitado (Dis).

L2 Only Indica si el direccionador está funcionando únicamente en el nivel 2, yes (verdad) o no (falso).

Ext Dom Indica si el direccionador está funcionando fuera del dominio de direccionamiento IS-IS (dominio externo).

Metric Indica el costo del uso de esta subred.

EIH Indica el intervalo de envío a la subred de los mensajes hello de ES.

IIH Indica el intervalo de envío de los mensajes hello de IS a la subred.

Ejemplo:

```
list subnet detailed
Interface Number [0]? 0

Detailed information for subnet 0:
  ISIS Level 1 Multicast: 018002B000014
  ISIS Level 2 Multicast: 018002B000015
  All ISs Multicast:      009002B000005
  All ESs Multicast:      009002B000004
  Level 1 Priority: 64
  Level 2 Priority: 64
```

ISIS Level 1 Multicast

Indica la dirección de difusión múltiple a usar cuando se transmitan y reciban PDU IS-IS de L1.

ISIS Level 2 Multicast

Indica la dirección de difusión múltiple a usar cuando se transmitan y reciban PDU IS-IS de L2.

All ISs Multicast

Indica la dirección de difusión múltiple a usar cuando se reciban hellos de ES.

All ESs Multicast

Indica la dirección de difusión múltiple a usar cuando se transmitan hellos de IS.

Level 1 Priority/Level 2 Priority

Indica la prioridad del direccionador para convertirse en el direccionador designado de la LAN.

templates

Muestra una lista de las plantillas de este direccionador.

Ejemplo:

```
list template
Route Cir Name      Template Name      DTE Addr      Call UserData
routetest2          temptest2          25             81
```

timers

Muestra la configuración del temporizador OSI/DNA V (qué se está ejecutando en el direccionador, OSI o DNA V).

Ejemplo:

```
list timers
Timers:
Complete SNP (sec) = 10      Partial SNP (sec) = 2
Min LSP Gen (sec) = 30      Max LSP Gen (sec) = 900
Min LSP Xmt (sec) = 30      Min Br LSP Xmt (msec) = 33
Waiting Time (sec) = 60     DR ISIS Hello (sec) = 1
ES Config Timer (sec) = 10
```

Timers: Indica la configuración de los temporizadores de OSI salvo los temporizadores por circuito.

Complete SNP

Intervalo entre la generación de SNP completos.

Partial SNP

Intervalo mínimo entre el envío de SNP parciales.

Min LSP Generation/Max LSP Generation

Los intervalos mínimo y máximo entre las generaciones de LSP.

Min LSP Transmission

El intervalo mínimo entre retransmisiones de LSP.

Mandatos de configuración de OSI/DECnet V (Talk 6)

Min Broadcast LSP Transmission

El intervalo mínimo entre retransmisiones LSP en un circuito de difusión.

Waiting Time

Tiempo de retardo del proceso de actualización antes de entrar en el estado ON (activo).

DR ISIS Hello

Intervalo entre generaciones de PDU de hello IS-IS si este direccionador es un direccionador designado.

ES Config Timer

Intervalo mínimo en el que un ES debe enviar un paquete hello cada vez que se activa una interfaz.

virtual-circuits

Muestra información sobre todos los circuitos virtuales X.25.

Ejemplo: `list virtual-circuits`

Set

Use el mandato **set** para configurar el direccionador para que ejecute el protocolo OSI.

Sintaxis:

set adjacency
 algorithm
 globals
 network-entity-title
 phaseivpfx
 subnet
 switches
 timers
 transmit-password (sólo configuración DEC)
 virtual-circuit (sólo configuración IBM 2210)

adjacency

Añade o cambia una adyacencia ES. Añade una adyacencia ES para todas las LAN ES que no ejecutan el protocolo ES-IS.

Ejemplo:

```
set adjacency
Interface Number [0]:
Area Address [ ]:
System ID [ ]:
MAC Address [ ]:
```

Interface Number

Indica el número de la interfaz que se conecta con la adyacencia.

Area Address

Indica el área donde está situada la adyacencia.

System ID

Indica la parte del ID del sistema del NET que se usa para identificar la adyacencia.

MAC Address

Indica la dirección de MAC (SNPA) de la adyacencia.

algorithm

Nota: Se trata de un mandato de DNA phase V. Este mandato sólo funcionará si se incluye el protocolo DNA phase V en la carga de software. Esto le permitirá seleccionar el tipo de algoritmo de direccionamiento que está usando para el protocolo de direccionamiento de DNA, el estado de enlace (DNA V) o el vector de distancia (DNA IV).

Ejemplo:

```
set algorithm
Level 1 Algorithm [link_state]?
Level 2 Algorithm [distance_vector]?
```

Level 1 Algorithm

Selecciona el tipo de algoritmo de direccionamiento, el link_state (estado_enlace) (para redes DNA V) o el distance_vector (vector_distancia) (para redes DNA IV).

Level 2 Algorithm

Selecciona el tipo de algoritmo de direccionamiento, el link_state (estado_enlace) (para redes DNA V) o el distance_vector (vector_distancia) (para redes DNA IV).

globals Configura los parámetros globales necesarios para el protocolo OSI.

Ejemplo:

```
set globals
IS Type [L2]:
System ID Length [6 bytes]:
Max Synonymous Areas [3]:
L1 LSP Buffer Size [1492 bytes]:
L2 LSP Buffer Size [1492 bytes]:
Max IS Adjacencies ]50[:
Max ES Adjacencies [200]:
Max Areas in Domain [50]:
Max ESs per Area [500]:
Max Internal Prefix Addresses [100]:
Max External Prefix Addresses [100]:
Max Link State Updates [100]?
```

IS Type (L1 o L2)

Selecciona el nivel del direccionador: nivel 1 o nivel 2.

System ID Length

Selecciona la longitud de la parte del ID de dominio del NET. Esta longitud debe ser la misma para todos los direccionadores del mismo dominio.

Max Synonymous Areas

Selecciona el número máximo de áreas de nivel 1 a las que sirve este direccionador.

L1 LSP Buffer Size

Selecciona el tamaño del almacenamiento intermedio de los SNP y LSP de nivel 1 originados por el direccionador. El rango está entre 512 y 1492. Si el tamaño del paquete de la interfaz es inferior al configurado aquí, OSI no se ejecutará y el direccionador generará el mensaje ELS ISIS.053.

L2 LSP Buffer

Selecciona el tamaño del almacenamiento intermedio de los SNP y los LSP de nivel 2 originados por el direccionador. El rango está entre 512 y 1492. Si el tamaño del paquete de la interfaz es inferior al configurado aquí, OSI no se ejecutará y el direccionador generará el mensaje ELS ISIS.053.

Max IS Adyacencias

Selecciona el número total de las adyacencias IS permitidas para todos los circuitos. Este número se usa para dar tamaño a la agrupación libre de adyacencias IS.

Max ES Adyacencias

Selecciona el número total de las adyacencias ES permitidas para todos los circuitos. Este número se usa para dar tamaño a la agrupación libre de adyacencias ES.

Max Areas in Domain

Selecciona el número total de áreas del dominio de direccionamiento. Este número se usa para dar tamaño a la tabla de direccionamientos L2.

Max ESs per Area

Selecciona el número total de ES en cualquier área. Este número se usa para dar tamaño a la tabla de direccionamientos L1.

Max Internal Reachable Addresses

Selecciona el número que está usando para dar tamaño a la tabla de direccionamientos métricos interna.

Max External Reachable Addresses

Selecciona el número que está usando para dar tamaño a la tabla de direccionamientos métricos externa.

Max Link State Updates

Selecciona el número que está usando para dar tamaño a la base de datos de estados de enlace.

network-entity-title

Configura el NET del direccionador. El NET está formado por el ID de sistema del direccionador y la dirección de área del direccionador.

Ejemplo:

```
set network-entity-title
Area-address [ ]
System-ID [ ]:
```

Area-address

Indica una de las porciones de dirección de área del NET del direccionador. Se incluye como primera dirección en el juego de direcciones de áreas manuales del direccionador. Cada dirección de área puede tener un máximo de 19 bytes.

System-ID

Define la parte del NSAP que identifica este direccionador específico. El ID del sistema puede tener un máximo de 19 bytes, pero la longitud debe estar de acuerdo con la longitud del ID de dominio configurada con el mandato **set globals**.

phaseivpfx

Configura la dirección-prefijo para permitir al protocolo OSI direccionar paquetes a la red DNA IV conectada. El valor por omisión es 49 (hexadecimal).

Ejemplo: **set phaseivpfx**

```
Local Phase IV prefix [49]?
```

subnet

Añade o cambia una subred. Este parámetro le solicita información diferente, según el tipo de subred que configure. X.25 o LAN.

Ejemplo:

Subred X.25:

```
set subnet
Interface number [0]:
Interface Type [X25]:
```

Subred LAN

```
Interface number [0]:
Interface Type [LAN]:
Enable ES-IS [N]?
Enable IS-IS [N]?
Level 2 Only [N]?
External Domain [N]?
Default Metric [20]:
ESIS IS Hello Timer [10 sec]:
ISIS Hello Timer [3 sec]:
Modify Transmit password [No]?
Modify the set of receive passwords [No]?
L1 Priority [64]:
L2 Priority [64]:
All ESs [0x09002B000004]:
All ISs [0x09002B000005]:
All L1 ISs [0x0180C2000014]:
All L2 ISs [0x0180C2000015]:
```

Subred Frame Relay:

```
Interface number [0]:
Interface Type [FRL]:
```

Interface number

Enlaza la subred con la interfaz especificada.

Enable ES-IS

Indica si el protocolo ES-IS va a ejecutarse sobre la interfaz, sí (Y) o no (N).

Enable IS-IS

Indica si el protocolo IS-IS va a ejecutarse sobre la interfaz, sí (Y) o no (N).

Interface Type

Indica el tipo de subred: LAN, X.25 y Frame Relay (FRL). LAN incluye Ethernet y red en anillo.

Level 2 Only

Indica si la subred debe ejecutarse sólo en nivel 2, sí (Y) o no (N). Un no permitirá al direccionador direccionar sobre la subred en el nivel 1 y el 2.

Mandatos de configuración de OSI/DECnet V (Talk 6)

External Domain

Indica si el circuito está funcionando fuera del dominio de direccionamiento IS-IS.

Default Metric

Indica el costo de la subred. El costo está en el rango incluido entre 20 y 63.

IS Hello Timer

Indica el período entre transmisiones de PDU de hello de IS.

ISIS Hello Timer

Indica el período de transmisiones de PDU de hello IS-IS de L1 y L2.

Modify Transmit password

Elimina o cambia una contraseña de transmisión de un circuito. Si selecciona yes (sí), esta opción le solicitará:

```
Delete or change the transmit password  
[change]?
```

Modify the set of receive passwords

Elimina todo o añade una contraseña de recepción de circuito. Si selecciona yes (sí), esta opción le solicitará:

```
Delete all or add 1 receive password  
[add]?
```

L1 Priority/L2 Priority

Indica la prioridad del direccionador para convertirse en el direccionador designado de la LAN.

All ESs

Indica la dirección de difusión múltiple a usar cuando se transmitan hellos de IS. La dirección por omisión refleja la dirección de difusión múltiple de ethernet/802.3. Si está conectándose con una 802.5 LAN, use **C00000004000**.

All ISs

Indica la dirección de difusión múltiple a usar cuando se reciban hellos de ES. La dirección por omisión refleja la dirección de difusión múltiple de ethernet/802.3. Si está conectándose con una 802.5 LAN, use **C00000008000**.

All L1 ISs

Indica la dirección de difusión múltiple a usar cuando se transmitan y reciban PDU IS-IS de L1. La dirección por omisión refleja la dirección de difusión múltiple de ethernet/802.3. Si está conectándose con una 802.5 LAN, use **C00000008000**.

All L2 ISs

Indica la dirección de difusión múltiple a usar cuando se transmitan y reciban PDU IS-IS de L2. La dirección por omisión refleja la dirección de difusión múltiple de ethernet/802.3. Si está conectándose con una 802.5 LAN, use **C00000008000**.

switches Activa y desactiva las opciones de OSI.

Ejemplo:

```
set switches  
ES-IS Checksum Option [OFF]?  
ES-IS Init Option [OFF]?  
ISIS Authentication [OFF]?
```

IS-IS Checksum Option

Cuando esta opción está activada, el direccionador genera sumas de comprobación para todos los paquetes ES-IS de origen.

ES-IS Init Option

Cuando esta opción está activada, el direccionador envía un hello de IS directo a un vecino ES nuevo.

IS-IS Authentication

Si esta opción está activada, cada paquete IS-IS incluye la contraseña de transmisión configurada para el dominio, el área y los circuitos. Además, no se comprueba con las contraseñas de recepción.

timers Configura los temporizadores de OSI, excluyendo los temporizadores de circuito.

Ejemplo:

set timers

Complete SNP [10 sec]:

Partial SNP [2 sec]:

Minimum LSP Generation [30 sec]:

Maximum LSP Generation [900 sec]:

Minimum LSP Transmission [5 sec]:

Minimum Broadcast LSP Transmission [33 msec]:

Waiting Time [60 sec]:

Designated Router ISIS Hello [1 sec]:

Suggested ES Configuration Timer (sec) [10]:

Complete SNP

Selecciona el intervalo transcurrido entre la generación de PDU de número de secuencia completos (SNP) por el direccionador designado en un circuito de difusión.

Partial SNP

Selecciona el intervalo mínimo entre el envío de PDU de número de secuencia parciales (SNP).

Minimum LSP Generation

Selecciona el intervalo mínimo entre generaciones sucesivas de paquetes de estado de enlace (LSP) con el mismo ID de LSP generado por el direccionador.

Maximum LSP Generation

Selecciona el intervalo máximo entre LSP generados por el direccionador.

Minimum LSP Transmission

Selecciona el intervalo mínimo entre retransmisiones de un LSP.

Minimum Broadcast LSP Transmission

Selecciona la transmisión mínima, en milisegundos, entre la transmisión de LSP en un circuito de difusión.

Waiting Time

Selecciona la cantidad de segundos que debe retardarse el proceso de actualización en el estado de espera antes de entrar en el estado ON (activo).

Mandatos de configuración de OSI/DECnet V (Talk 6)

Designated Router ISIS Hello

Selecciona el intervalo transcurrido entre la generación de PDU de hello IS-IS por parte del direccionador, si éste es el direccionador designado de una LAN.

Suggested ES Configuration Timer

Establece el campo de opción del mensaje hello de IS que instruye al ES que cambie el ritmo de envío de hellos de ES.

transmit-password

Establece o cambia una contraseña de transmisión.

Ejemplo:

```
set transmit-password
Password type [Domain]:
Password [ ]:
Reenter password:
```

Password type

Selecciona el tipo de contraseña: *dominio* o *área*.

Las contraseñas de dominio se usan con SNP y LSP de L2. Las contraseñas de área se usan con LSP L1 y SNP.

Password

Indica la serie de caracteres que se usa para autenticación. La serie de caracteres máxima permitida puede tener 16 caracteres.

virtual-circuit

Configura un SVC o PVC X.25 o un PVC Frame Relay.

Ejemplo:

```
set virtual-circuit
Interface Number [0]:
DTE Address[]:
Enable ISIS (Y or N) [Y]?
L2 only (Y or N) [N]?
External Domain (Y or N) [N]?
Default Metric [20]:
ISIS Hello Timer [3 sec]?
Modify transmit password (y or n) [N]?
Modify the set of receive passwords [No]?
```

Interface Number

Indica la interfaz de X.25 o de Frame Relay sobre la que está configurado el circuito virtual.

DTE Address

Indica la dirección del DTE de destino para X.25 o el DLCI (identificador de control del enlace de datos) para Frame Relay. Esta dirección debe ser la misma que la definida para el circuito virtual en la configuración de X.25 o en la de Frame Relay.

Default Metric

Indica el costo del circuito.

Enable IS-IS

Indica si el protocolo IS-IS va a ejecutarse sobre la interfaz, sí (Y) o no (N).

L2 only Indica si el circuito debe ejecutarse sólo en el nivel 2, yes (Y) o no (N). Un no permitirá al direccionador direccionar en el nivel 1 y el nivel 2.

External Domain

Indica si el circuito está funcionando fuera del dominio de direccionamiento IS-IS.

Acceso al entorno de supervisión de OSI/DECnet V

Si desea obtener información sobre cómo acceder al entorno de supervisión de OSI/DECnet V, consulte *Getting Started (Introduction to the User Interface)* en el manual *Guía del usuario de software*

Mandatos de supervisión de OSI/DECnet V

Esta sección describe los mandatos de supervisión de OSI/DECnet V. Use estos mandatos para reunir información de la base de datos.

Los mandatos de supervisión muestran o modifican la base de datos volátil.

<i>Tabla 108 (Página 1 de 2). Resumen de los mandatos de supervisión de OSI/DECnet V</i>	
Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte la sección "Cómo obtener ayuda" en la página xxix.
Addresses	Muestra las direcciones de área y NET del direccionador.
Change Metric	Modifica el costo de un circuito.
CLNP-Stats	Muestra estadísticas OSI CLNP.
DNAV-info	Muestra el algoritmo de direccionamiento de nivel 1 y nivel 2 que actualmente está en vigor.
Designated-router	Muestra el direccionador designado de la LAN.
ES-adjacencies	Muestra todas las adyacencias de ES de la base de datos de adyacencias.
ES-IS-Stats	Muestra las estadísticas asociadas al protocolo ESIS.
IS-adjacencies	Muestra todas las adyacencias IS de la base de datos de adyacencias.
IS-IS-Stats	Muestra las estadísticas asociadas al protocolo ISIS.
L1-routes	Muestra todas las rutas de L1 de la base de datos de nivel 1.
L2-route	Muestra todas las rutas de L2 de la base de datos de nivel 2.
L1-summary	Muestra un resumen de la base de datos de enlaces de nivel 1.
L2-summary	Muestra un resumen de la base de datos de enlaces de nivel 2.
L1-update	Muestra la información contenida en el paquete de actualización de estado de enlace de L1.
L2-update	Muestra la información contenida en el paquete de actualización de estado de enlace de L2.

Mandatos de supervisión de OSI/DECnet V (Talk 5)

Tabla 108 (Página 2 de 2). Resumen de los mandatos de supervisión de OSI/DECnet V	
Mandato	Función
Ping-1139	Hace que el direccionador envíe una solicitud de eco a un destino y espere una respuesta.
Route	Muestra la ruta que sigue un paquete hasta un destino especificado.
Send echo packet	Codifica un mensaje de solicitud de eco en el paquete CLNP.
Show routing circuits	Muestra el estado de los circuitos de direccionamiento definidos por el usuario para una interfaz especificada. Se aplica cuando el direccionador está configurado como un direccionador de estilo DEC.
Subnets	Muestra todas las subredes definidas por el usuario.
Toggle	Habilita o inhabilita la función de sustitución de alias NSAP.
Traceroute	Muestra la ruta que sigue un paquete hasta su destino.
Virtual-circuits	Muestra todos los circuitos virtuales definidos por el usuario. Se aplica cuando el direccionador está configurado como un direccionador de estilo IBM 2210.
Exit	Le devuelve al nivel de mandatos anterior. Consulte la sección "Cómo salir de un entorno de nivel inferior" en la página xxix.

Addresses

Use el mandato **addresses** para establecer una lista de las direcciones de área y NET del direccionador que están configuradas.

Sintaxis:

addresses

Ejemplo:

```
addresses
Network Entity Title:
4700-0500-01 000-9310-04F0
Area Addresses:
4700-0500-01
4900-02
```

Network Entity Title

Identifica al direccionador. El NET está formado por una dirección de área y un ID de sistema.

Area Address

Indica las direcciones dentro del dominio de direccionamientos. El direccionador puede tener un máximo de tres direcciones de área configuradas al mismo tiempo.

Change Metric

Use el mandato **change metric** para modificar el costo de un circuito.

Sintaxis:

change metric

Ejemplo:

```
change metric
Circuit [0]?
New Cost [0]?
```

Circuit Indica el número del circuito que desea cambiar.

New Cost

Indica el costo nuevo del circuito. Rango: De 1 a 63.

CLNP-Stats

Use el mandato **clnp-stats** para visualizar las estadísticas de OSI Connectionless Layer Network Protocol (CLNP).

Sintaxis:clnp-statistics**Ejemplo:****clnp-statistics**

```
Received incomplete packet          0
Received packet with bad NSAP length 0
Received packet with bad checksum   0
Received packet with bad version number 0
Received packet with bad type       0
Received packet with expired lifetime 0
Received packet with bad option     0
Received packet with unknown destination 0
Received packet with no segmentation permitted 0
Received data packet cannot be forwarded 0
CLNP input queue overflow           0
No buffer available to send error packet 0
No route to send error packet       0
Received OK CLNP packet             0
Cannot forward error packet         0
ISO unknown initial protocol ID     0
Received error packet               0
Received local data packet          0
Sent error packet                   0
received echo packet - destination unknown 0
cannot send an echo packet, handler error 0
sent ECHO reply packet              0
sent ECHO request packet            0
received ECHO Request                0
received ECHO reply                  0
Error PDU dropped - SP, MS or E/R flag set 0
```

Received incomplete packet

Indica que se ha recibido un fragmento de un paquete de datos que se ha reconocido como un paquete de datos ISO CLNP.

Received packet with bad NSAP length

Indica que se ha recibido un paquete de datos ISO CLNP con una longitud NSAP incorrecta.

Received packet with bad checksum

Indica que se ha recibido un paquete de datos ISO CLNP con una suma de comprobación errónea.

Received packet with bad version number

Indica que se ha recibido un paquete de datos ISO CLNP con un número de versión sin soporte o incorrecto.

Mandatos de supervisión de OSI/DECnet V (Talk 5)

Received packet with bad type

Indica que se ha recibido un paquete de datos ISO CLNP con un campo de tipo sin soporte o incorrecto.

Received packet with expired lifetime

Indica que se ha recibido un paquete de datos ISO CLNP con un tiempo de vida agotado.

Received packet with bad option

Indica que se ha recibido un paquete de datos ISO CLNP con un parámetro opcional erróneo.

Received packet with unknown destination

Indica que se ha recibido un paquete de datos ISO CLNP pero que no se ha podido direccionar. La tabla de direccionamientos no contiene una entrada para el destino.

Received packet with no segmentation permitted

Indica que se ha recibido un paquete de datos ISO CLNP que necesitaba segmentación. El distintivo de segmentación permitido no está establecido.

Received data packet cannot be forwarded

Indica que se ha recibido un paquete de datos ISO CLNP pero que no se ha podido direccionar debido a un error del manejador.

No buffer available to send error packet

Ha fallado un intento de enviar un paquete de error ISO CLNP debido a una falta de almacenamientos intermedios de E/S del sistema.

No route to send error packet

Ha fallado un intento de enviar un paquete de error ISO CLNP porque no se ha podido direccionar.

Received OK CLNP packet

Indica que se ha recibido un paquete de datos ISO CLNP y que éste ha pasado la comprobación de errores.

Cannot forward error packet

Indica que no se ha podido direccionar un paquete de error ISO CLNP debido a un error del manejador.

ISO unknown initial protocol ID

Indica que se ha recibido un paquete ISO CLNP con un identificador de protocolo inicial sin soporte o desconocido.

Received error packet

Indica que se ha recibido un paquete de error ISO CLNP para este direccionador.

Received local data packet

Indica que se ha recibido un paquete de datos ISO CLNP con un NSAP de destino que indica uno de los NSAP del direccionador.

Sent error packet

Indica que se ha enviado un paquete de error ISO CLNP al recibir un paquete anómalo.

Designated-router

Use el mandato **designated-router** para visualizar el direccionador designado para las subredes LAN que están conectadas físicamente a este direccionador y ejecutan activamente IS-IS.

Sintaxis:

designated-router

Ejemplo:

```
designated-router
Designated Router Information:
Hdw  Int#  Circ   L1DR                               L2DR
Eth/1 1     2     0000931004F002                    0000931004F002
TKR/0 0     1     Elvis-01                          Elvis-01
```

Hdw Indica el tipo e instancia de la LAN conectada a este direccionador.

Intnúm. Indica el número de la interfaz de este direccionador que establece una conexión con la LAN.

Circ Indica el número de circuito asignado por el direccionador. Este valor siempre es un número más que el número asignado a la interfaz para las subredes de la LAN.

L1DR Indica el ID de LAN del direccionador designado. Si está habilitado el uso de un alias, este mandato visualizará el alias del segmento en concreto. El ID de LAN es el ID del sistema del direccionador designado concatenado con un ID de circuito asignado localmente de 1 byte.

L2DR La descripción de este parámetro es la misma que para el parámetro L1DR anterior.

Nota: Si todavía no se ha elegido el direccionador designado, aparecerá "Not Elected" (Sin elegir) en vez de un ID de LAN.

DNAV-info

Use el mandato **dnav-info** para visualizar el algoritmo de direccionamiento que está ejecutándose actualmente en el direccionador.

Sintaxis:

dnav-info

Ejemplo:

```
dnav-info
DNA V Level 1 Routing Algorithm: Distance-vector
DNA V Level 2 Routing algorithm: Distance-vector
```

Nota: Según si DNA IV está habilitado o no, el algoritmo que aparezca aquí puede diferir de lo que se haya configurado en memoria con el mandato **set algorithm** en el indicador `config>` de OSI/DECnet V.

Si DNA IV está habilitado - el algoritmo de direccionamiento será el que esté configurado en memoria.

Si DNA IV está inhabilitado - el algoritmo de direccionamiento se establecerá en estado de enlace y puede ser diferente del que se haya establecido en memoria.

ES-Adyacencias

Use el mandato **es-adjacencias** para visualizar todas las adyacencias del sistema final (ES) que estén configuradas o se hayan sabido a través del protocolo ESIS.

Sintaxis:

es-adjacencias

Ejemplo:

```
es-adjacencias
End System Adjacencies
System ID      MAC Address      Interface  Lifetime  Type
6666-6666-6666 1234-FEAA-041C      0          50        DNAIV
```

System ID

ID del sistema de la adyacencia ES.

MAC Address

Indica la dirección del MAC del ES de la subred.

Interface Indica el número de la interfaz del direccionador donde se tuvo conocimiento de la adyacencia ES.

Lifetime Indica el período de tiempo, en segundos, que el direccionador ha dejado antes de que se descarte la información recibida en el último mensaje ES Hello. En el caso de una ES-Adjacency (adyacencia ES) configurada estática o manualmente, este campo lee **Static**.

Type Indica el tipo de adyacencia ES, OSI DNAIV, DNAIV' y MANUAL para las adyacencias configuradas estáticamente.

ES-IS-Stats

Use el mandato **es-is-stats** para visualizar las estadísticas del protocolo ESIS.

Sintaxis:

es-is-stats

Ejemplo:

es-is-stats

ESIS input queue overflow	0
Received incomplete packet	0
Received packet with bad checksum	0
Received packet with bad version	0
Received packet with bad type	0
No iob available to send hello	0
Cannot send hello due to packet handler error	0
Sent hello	3672
Received packet with bad header	0
Received hello with bad nsap	0
Received hello packet with bad option	0
Received hello	0
Received hello with unsupported domain source	0
No resources to install route	0
Received hello with conflicting route	0
Timed out route reactivated	0
No resources to send redirect	0
Redirect not sent - handler error	0
Sent redirect	0
Timed out route	0
Timed out route	0
Unable to allocate resources for a new ES adjacency	0
hello PDU dropped, received over point-to-point circ	0
ESIS hello PPDU dropped, no matching area address	0
dropped hello packet - manual ES adjacency exists	0

ESIS input queue overflow

El paquete ESIS se ha eliminado debido a que se ha desbordado una cola de entrada de tareas.

Received incomplete packet

Se ha recibido un fragmento de paquete reconocido como un paquete ESIS.

Received packet with bad checksum

Se ha recibido un paquete ESIS con una suma de comprobación errónea.

Received packet with bad version

Se ha recibido un paquete ESIS con una versión sin soporte o errónea.

Received packet with bad type

Se ha recibido un paquete ESIS con un campo de tipo sin soporte o erróneo.

No iob available to send hello

Ha fallado un intento de enviar un paquete hello de ESIS debido a una falta de almacenamientos intermedios de E/S del sistema.

Cannot send hello due to packet handler error

No se ha podido enviar un hello de ESIS debido a un error del manejador.

Sent hello

Se ha enviado un hello de ESIS a una interfaz.

Received packet with bad header

Se ha recibido un paquete hello de ESIS con un tiempo de retención o un campo recibido erróneo.

Received hello with nsap

Se ha recibido un paquete hello de ESIS con un NSAP erróneo o un NSAP que desborda el campo.

Mandatos de supervisión de OSI/DECnet V (Talk 5)

Received hello packet with bad option

Se ha recibido un paquete de datos ESIS CLNP con un parámetro de opción erróneo.

Received hello

Se ha recibido en la interfaz un paquete hello de ESIS.

Received hello with unsupported domain source

Se ha recibido un paquete hello de ESIS proveniente de una fuente de dominio sin especificar.

No resources to install route

Se ha recibido un paquete hello de ESIS, pero no había recursos para instalar el direccionador.

Received hello with conflicting route

Se ha recibido un paquete hello de ESIS, pero no se ha podido entrar en la base de datos. Una ruta dinámica o estática definida anteriormente en la base de datos entra en conflicto con la ruta del hello.

Timed out route reactivated

Se ha recibido un paquete hello de ESIS con una ruta con tiempo excedido previamente.

No resources to send redirect

No se ha podido enviar un paquete de redirección ESIS debido a falta de recursos.

Redirect not sent handler error

No se ha podido enviar un paquete de redirección ESIS debido a un error del manejador.

Sent redirect

Se ha enviado a la interfaz un paquete de redirección de ESIS.

Timed out route

Una ruta hello de ESIS ha excedido el tiempo.

Unable to allocate resources for a new ES adjacency

Se ha recibido un paquete hello de ES-IS pero el direccionador no tiene los recursos suficientes para establecer una adyacencia de ES con el nodo transmisor.

hello PDU dropped, received over point-to-point circ

Se ha eliminado un paquete hello de ES-IS debido a que el circuito implicado es un circuito de punto a punto.

ESIS hello PDU dropped, no matching area address

Se ha eliminado un paquete hello de ES-IS debido a que el área no coincidía con la dirección de área del direccionador. El protocolo ES-IS sólo se aplica a un área.

dropped hello packet-manual ES adjacency exists.

Se ha eliminado un paquete hello de ES-IS debido a que existe una adyacencia de ES estática con el nodo transmisor.

IS-Adjacencies

Use el mandato **IS-adjacencies** para establecer una lista de todas las adyacencias IS de las que se tiene conocimiento a través del protocolo ISIS.

Sintaxis:

is-adjacencies

Ejemplo:

```
is-adjacencies
Intermediate System Adjacencies
System ID      MAC Address    Int  Level Usage  State  Life  Type
0000-9310-04C8 AA00-0400-EF04 0    L1   L1/L2 DOWN   5390  OSI
0000-9310-04C8 AA00-0400-EF04 0    L2   L1/L2 DOWN   5390  DNAIV
AA00-0400-0504 AA00-0400-0504 1    L2   L2     UP     5390  OSI
```

System ID

EL ID del sistema de la adyacencia IS.

MAC Address

Indica la dirección del MAC de la adyacencia IS.

Int Indica el número de la interfaz del direccionador que establece la conexión con la adyacencia IS.

Level En el caso de las LAN, este parámetro indica el nivel del sistema vecino a partir del tipo de mensaje hello, L1 o L2. Para punto a punto, indica sólo el tipo de sistema vecino L1, de lo contrario L2.

Usage Indica, a partir del tipo de circuito del paquete hello, sólo L1, sólo L2 o L1 y L2.

State Indica el estado operacional de la adyacencia IS, activa o inactiva.

Life Indica el período de tiempo, en segundos, que tiene que transcurrir para descartar el último mensaje hello de IS.

Type Indica el tipo de protocolo de direccionamiento de la adyacencia IS, OSI o DNA IV.

IS-IS-Stats

Use el mandato **is-is-stats** para visualizar la información asociada al protocolo ISIS.

Sintaxis:

is-is-stats

Ejemplo:

Mandatos de supervisión de OSI/DECnet V (Talk 5)

is-is-stats

Link State Database Information

no. of level 1 LSPs	1	no. of level 2 LSPs	0
no. of L1 Dijkstra runs	21	no. of L2 Dijkstra runs	0
no. of L1 LSPs deleted	0	no. of L2 LSPs deleted	0
no. of routing table entries allocated	6		

Packet Information

level 1 lan hellos rcvd	0	level 1 lan hellos sent	10967
level 2 lan hellos rcvd	0	level 2 lan hellos sent	10967
pnt to pnt hellos rcvd	0	pnt to pnt hellos sent	0
level 1 LSPs rcvd	0	level 1 LSPs sent	40
level 2 LSPs rcvd	0	level 2 LSPs sent	0
level 1 CSNPs rcvd	0	level 1 CSNPs sent	0
level 2 CSNPs rcvd	0	level 2 CSNPs sent	0
level 1 PSNPs rcvd	0	level 1 PSNPs sent	0
level 2 PSNPs rcvd	0	level 2 PSNPs sent	0

no. of level 1/level 2 LSPs

Indica el número de paquetes de estado de enlace L1 y L2 que hay en la base de datos.

no. of L1/L2 Dijkstra runs

Indica el número de veces que el direccionador calculó las tablas de direccionamiento L1 y L2.

no. of L1/L2 LSPs deleted

Indica el número de paquetes de estado de enlace L1 y L2 que se suprimieron de la base de datos.

no. of routing table entries allocated

Indica el número de entradas que contiene actualmente la tabla de direccionamientos.

level 1/level 2 lan hellos rcvd

Indica el número de hellos de LAN que el direccionador ha recibido.

level 1/level 2 hellos sent

Indica el número de hellos de LAN que el direccionador ha enviado.

pnt to pnt hellos rcvd

Indica el número de hellos de punto a punto que el direccionador ha recibido.

pnt to pnt hellos sent

Indica el número de hellos de punto a punto que el direccionador ha enviado.

level 1/level 2 LSPs rcvd

Indica el número de paquetes de estado de enlace (LSP) L1 y L2 que el direccionador ha recibido.

level 1/level 2 LSPs sent

Indica el número de LSP L1 y L2 que el direccionador ha enviado.

level 1/level 2 CSNPs rcvd

Indica el número de PDU de número de secuencia completa (CSNP) L1 y L2 que ha recibido el direccionador.

level 1/level 2 CSNPs sent

Indica el número de CSNP L1 y L2 que el direccionador ha enviado.

level 1/level 2 PSNPs rcvd

Indica el número de PDU de número de secuencia parcial L1 y L2 (PSNP) que ha recibido el direccionador.

level 1/level 2 PSNPs sent

Indica el número de PSNP L1 y L2 que el direccionador ha enviado.

L1-Routes

Use el mandato **I1-routes** para visualizar todas las rutas de nivel 1 que están en la base de direccionamientos L1.

Sintaxis:

I1-routes

Ejemplo:

I1-routes

Level 1 Routes	Destination System ID	Cost	Source	Next Hop
0000-9300-0047	0000-9300-0047	0	LOCAREA	*
AA00-0400-080C	AA00-0400-080C	1	ESIS	AA00-0400-0C04, Ifc 7
7777-7777-7777	7777-7777-7777	0	ISIS	3455-6537-2215

Destination System ID

Indica el ID del sistema del sistema principal de destino.

Cost Indica el costo de esta ruta.

Source Indica uno de los tres orígenes donde el direccionador tuvo conocimiento de la ruta: LOCAREA, ESIS o ISIS.

Next Hop Indica el salto siguiente que daría un paquete en su ruta. Una designación efectuada con un asterisco (*) se refiere al mismo direccionador como el destino del paquete. Una dirección con un número de interfaz es la dirección del MAC de un ES conectado directamente o la dirección del DTE si el salto siguiente es una conmutación X.25 o un DLCI si el salto siguiente es una conmutación Frame Relay. Un ID de sistema (34555372215) se refiere al salto siguiente hacia el destino.

L2-Routes

Use el mandato **I2-routes** para visualizar todas las rutas de nivel 2 de la base de datos de L2.

Sintaxis:

I2-routes

Ejemplo:

I2-routes

Level 2 Routes	Destination	Cost	Type	Next Hop
4700-0500-01	4700-0500-01	0	LOC-AREA	*
4900-02	4900-02	20	AREA	0000-9310-04C9

Destination

Indica el ID del sistema del área de destino o la dirección a alcanzar.

Cost Indica el costo de esta ruta.

Mandatos de supervisión de OSI/DECnet V (Talk 5)

- Type** Indica los cuatro tipos de rutas: área-LOC (local), prefijo-LOC, área, prefijo/I y prefijo/E. Área-LOC es un área conectada directamente; un prefijo-LOC es un prefijo que anuncia este direccionador; prefijo/I y prefijo/E son rutas que requieren otro salto para alcanzar su destino.
- Next Hop** Indica el salto siguiente que daría un paquete en su ruta. Una designación * o una designación directa, se refiere a un sistema principal conectado directamente fuera del direccionador. Un ID del sistema se refiere al siguiente direccionador por el que deberá pasar un paquete para alcanzar su destino.

L1-Summary

Use el mandato **l1-summary** para mostrar un resumen de la base de datos de estados de enlaces de nivel 1.

Sintaxis:

l1-summary

Ejemplo:

l1-summary

Link State Database Summary - Level One

LSP ID	Lifetime	Sequence #	Checksum	Flags	Cost
0000-9300-40B0-0000	0	0	0	0	1024
0000-93E0-107A-0000	384	CE	3CC9	1	0
AA00-0400-0504-0000	298	8E	40F1	B	20
AA00-0400-0504-0100	4	B8	A812	3	20

Total Checksum 25CC

LSP ID Representa el ID del sistema de origen de la PDU del estado de enlace más dos bytes adicionales. El primer byte adicional designa el tipo de actualización. 00 representa una actualización que no es un pseudonodo. 01–FF representa una actualización de pseudonodo para el número del circuito. El segundo byte representa el número de LSP. Este número se asigna al paquete cuando los datos están contenidos en más de un paquete.

Lifetime Indica el período de tiempo, en segundos, durante el cual el direccionador mantendrá el LSP.

Sequence #

Indica el número de secuencia del LSP.

Checksum

Indica el valor de la suma de comprobación del LSP.

Flags

Indica un valor de un octeto que refleja el campo del distintivo del LSP. Los ocho bits se desglosan como indicamos a continuación:

Bit 8 Indica el distintivo P. Cuando está establecido (1), el IS de emisión da soporte a la función Partition Repair (reparación de partición) opcional.

Bits 7-4 Indica el distintivo ATT. Cuando está establecido (1), el IS de emisión está conectado a otras áreas con una de las opciones siguientes: Default Metric (Métrica por omisión) (bit 4), Delay Metric (Métrica de retardo) (bit 5), Expense Metric

(Métrica de gastos) (bit 6) o Error Metric (Métrica de errores) (bit 7).

Bit 3 Indica el distintivo LSPDBOL. Cuando está establecido (1), se ha producido una sobrecarga de la base de datos de LSP. El proceso de decisión no usará el LSP que tenga este bit establecido para calcular rutas a otro l a través del sistema de origen.

Bits 2-1 Indica el distintivo del tipo de IS. Cuando se establece en los valores siguientes, designa el tipo de direccionador IS, nivel 1 o nivel 2.

Valor	Descripción
0	Sin usar.
1	Bit 1 establecido. IS de nivel 1.
2	Sin usar.
3	Bits 1 y 2 establecidos. IS de nivel 2.

Cost Indica el costo de direccionar a dicho vecino.

L2-Summary

Use el mandato **l2-summary** para visualizar un resumen de la base de datos de estados de enlace de nivel 2.

Sintaxis:

l2-summary

Ejemplo:

l2-summary

Link State Database Summary - Level Two

LSP ID	Lifetime	Sequence #	Checksum	Flags	Cost
0000-9310-04F0-0000	33E	12	EF19	3	0
0000-5000-FB06-0000	455	4	2BB1	3	20
0000-5000-FB06-0100	469	12	DE32	3	20

Total Checksum 0

La descripción de la producción de L2-summary es la misma que la del mandato l1-summary.

L1-Update

Use el mandato **l1-update** para visualizar una actualización del estado de enlace para el IS de nivel 1 especificado.

Sintaxis:

l1-update

Ejemplo:

Mandatos de supervisión de OSI/DECnet V (Talk 5)

l1-update

LSP ID []? 0000931004F0000

Link State Update For ID 0000931004F00000

Area Addresses

470005001

Intermediate System Neighbors	Metric	Two Way
0000931004F002	20	N
0000931004F001	20	Y

End System Neighbors	Metric
0000931004F0	*

LSP ID Indica el ID del sistema de origen de la PDU del estado de enlace más dos bytes adicionales. El primer byte designa el tipo de actualización. 00 representa una actualización que no es pseudonodo. 01–FF representa una actualización de pseudonodo. El segundo byte representa el número de LSP. Este número se asigna al paquete cuando los datos están contenidos en más de un paquete.

Area Addresses

Indica las direcciones del área donde este direccionador está configurado para direccionar paquetes.

Intermediate System Neighbors

Indica los IS vecinos adyacentes.

Metric Indica el costo del IS vecino.

Two Way Indica si el direccionador recibe actualizaciones del vecino.

End System Neighbors

Indica los ES conectados directamente.

L2-Update

Use el mandato l2-update para visualizar la actualización del estado del enlace para el IS de nivel 2 especificado.

Sintaxis:

l2-update

Ejemplo:

l2-update

LSP ID []? 0000931004F0000

Link State Update For ID 0000931004F00000

INTERMEDIATE SYSTEM NEIGHBORS	METRIC	TWO WAY
0000931004F002	20	N
0000931004F001	20	N
55002000182000	20	N

Intermediate System Neighbors

Indica otros IS conectados directamente.

Metric Indica el costo hasta el IS.

Two Way Indica si el direccionador recibe actualizaciones del vecino.

Ping-1139

Hace que el direccionador envíe una solicitud de eco a un destino y espere una respuesta, tal como se recomienda en RFC 1139. RFC 1139 especifica que esto es una función de OSI y no de DECnet. **Ping-1139** da soporte a ecos de corto y largo plazo. Los ecos de corto plazo usan paquetes de datos CLNP normales, lo que los convierte en transparentes para los sistemas intermedios que no dan soporte a RFC1139. Los ecos de largo plazo usan paquetes de solicitud/respuesta PING.

La longitud de los datos por omisión del paquete de solicitud de eco es de 16 bytes. Puede establecer la longitud de los datos hasta un máximo de 64 bytes.

Cuando entre el mandato **ping-1139**, las solicitudes de eco se enviarán continuamente hasta que pulse cualquier tecla. En ese momento, se visualizarán estadísticas en las que se verá el número de solicitudes transmitidas y el de respuestas recibidas.

Sintaxis:

ping-1139

Ejemplo:

```
ping-1139
Long-term/Short-term [LONG-TERM]?
Destination NSAP: []? AA0003000A14
Data Length [16]?

PINGing AA0003000A14

---- PING Statistics ----
 8 requests transmitted, 8 replies received
```

Route

Use el mandato **route** para visualizar el salto siguiente del paquete a un destino especificado (*destnsap*).

Sintaxis:

route *dest-nsap*

Ejemplo:

```
route 490002aa0004000e08
Destination System: 0000-9310-04C9
Destination MAC Address: AA00-0400-1408
Interface: 0
```

Destination System

Indica el ID del sistema del IS del salto siguiente. En el caso de un ES conectado directamente, este valor estará en blanco.

Destination MAC Address

Indica la dirección del MAC del IS del salto siguiente o el ES conectado directamente.

Interface Indica la interfaz que atravesará un paquete para llegar al IS del salto siguiente o al ES conectado directamente.

Send (Echo Packet)

Use el mandato **send echo packet** para codificar un mensaje de solicitud de eco en el paquete CLNP al nsap de destino especificado. Durante este mandato, el sistema no interactúa con la supervisión de OSI. Para verificar que se envió la solicitud de eco y que se recibió una respuesta de eco, compruebe el ELS (Sistema de anotación cronológica de sucesos).

Nota: No puede enviarse a sí mismo un paquete eco. Si lo intenta, recibirá un mensaje CLNP.004 ELS.

Sintaxis:

send

Ejemplo:

```
send
Destination NSAP: []?
```

Subnets

Use el mandato **subnets** para visualizar información sobre todas las subredes operacionales. Las subredes desactivadas o inhabilitadas no estarán en la lista.

Sintaxis:

subnets

Ejemplo:

```
subnets
L2
Hdw  Int #  Circ  Only  ES-IS  IS-IS  L1DR  L1Pri  L2DR  L2pri  Cost  Ext
PPP/2 2      3    N     N     Y
Eth/0 0      1    N     Y     Y     Y    64    N     64    20    N
```

Hdw El tipo e instancia de la red que conecta con la subred.

Int # El número de interfaz del direccionador que establece la conexión con la subred.

Circ El ID asignado al circuito para el protocolo ISIS.

L2 only Indica si este direccionador es sólo de nivel 2, Y (sí) o N (no).

ES-IS El protocolo ES-IS está habilitado en la subred, Y o N.

IS-IS El protocolo IS-IS está habilitado en la subred, Y o N.

L1DR Este direccionador es el direccionador designado de nivel 1 para esta subred, Y o N.

L1Pri La prioridad de nivel 1 de la subred de LAN para convertirse en el direccionador designado.

L2DR Este direccionador es el direccionador designado de nivel 2 para esta subred, Y o N.

L2Pri La prioridad de nivel 2 de la subred para convertirse en el direccionador designado.

Cost El costo del circuito.

Ext Indica si la subred trabaja fuera del dominio de direccionamiento IS-IS (externo).

Toggle (Alias/No Alias)

Use el mandato **toggle** alias/no alias para habilitar o inhabilitar la función de visualización del alias del NSAP para el protocolo OSI.

Sintaxis:

toggle

Ejemplo:

```
toggle
Alias substitution is ON
```

Traceroute

Use el mandato **traceroute** para rastrear la vía de acceso que sigue un paquete OSI hasta un destino.

Nota: No puede ejecutar un mandato traceroute hacia sí mismo, de lo contrario recibirá el mensaje de error siguiente:

```
Sorry, can't traceroute to this router. (No se
puede ejecutar un traceroute a este direccionador).
```

Sintaxis:

traceroute *dirección*

Ejemplo:

```
traceroute 490002aa0004000e08
Successful trace:
```

```
TRACEROUTE 470007: 56 databytes
```

```
1          490002aa0004000e08      32ms      5ms      5ms
```

```
Destination unreachable response:
```

```
Destination unreachable
```

```
No response:
```

```
1 * * *
2 * * *
```

TRACEROUTE

Muestra la dirección del área de destino y el tamaño del paquete que se envía a dicha dirección.

- 1** El primer rastreo que muestra el NSAP de destino y el tiempo que ha sido necesario para que el paquete llegase a su destino. El paquete se rastrea tres veces.

Destination unreachable

Indica que no hay ninguna ruta disponible al destino.

```
1 * * *
```

- 2 * * *** Indica que el direccionador está esperando algún tipo de respuesta del destino, pero que éste no responde. El direccionador esperará 32 saltos antes de considerar la condición de tiempo excedido. Vaya al ELS y active los mensajes OSI CLNP para determinar por qué el sistema principal no responde.

Uso de NHRP

Este capítulo describe cómo usar:

- Next Hop Resolution Protocol (NHRP) tal como se especifica en el Internet Draft Version 13, que se ha presentado para obtener el estado de RFC.

Visión general de Next Hop Resolution Protocol (NHRP)

Next Hop Resolution Protocol (NHRP) define un método para que una estación de origen determine la dirección de acceso múltiple sin difusión (NBMA) del “salto siguiente” hacia el destino. El siguiente salto NBMA puede ser el mismo destino o el direccionador de salida de la red NBMA “más cercana” a la estación de destino. Esta información del “salto siguiente” se llama ruta de atajo (“cut-through”) o VC en la especificación NHRP; el direccionador usa el término “shortcut” en vez de “cut-through”. La estación de origen puede establecer el circuito virtual NBMA directamente con el destino o el direccionador de salida y reducir el número de saltos en la red.

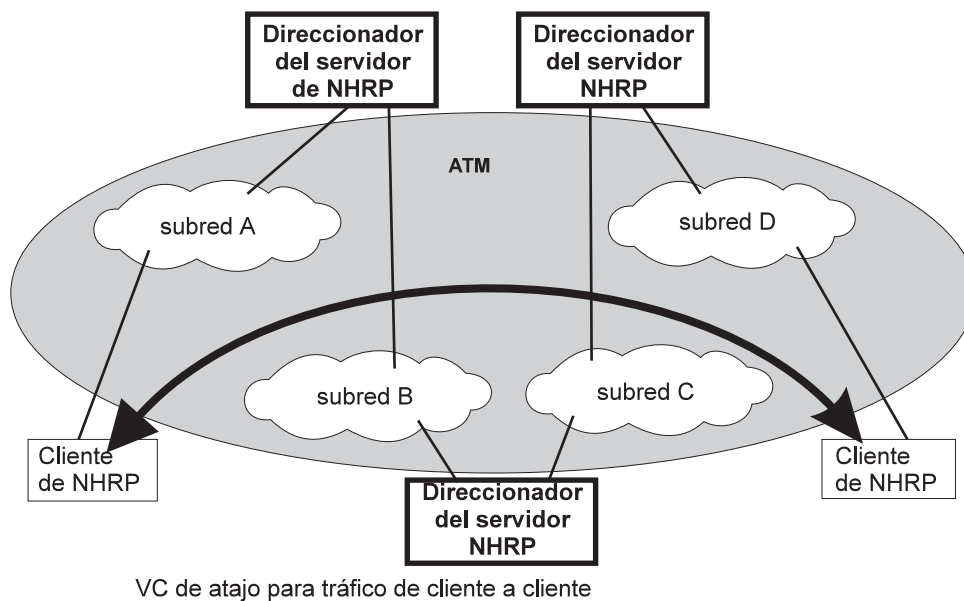


Figura 26. Visión general de Next Hop Resolution Protocol (NHRP)

El 2210 puede usar NHRP para establecer atajos para tráfico IP sobre la red ATM NBMA para interfaces RFC 1483 y Emulated LAN (ELAN). El borrador de Internet no trata el uso de NHRP en el entorno ELAN, pero el 2210 incluye mejoras para permitir usar LAN. Estas mejoras se implementan actualmente usando las extensiones propias de cada proveedor incluidas en la definición del protocolo NHRP.

El borrador de NHRP describe el flujo de protocolo básico como sigue: los clientes de NHRP registran sus direcciones de protocolo y las direcciones de NBMA en uno o varios servidores de NHRP. Por lo general, los servidores son direccionadores de la vía de acceso direccionada a través de la red NBMA a los clientes. Cuando un cliente desea establecer un atajo a un destino, envía un paquete Next Hop Resolution Request (Solicitud de resolución de salto siguiente) por la vía de acceso direccionada. La solicitud incluye la dirección del protocolo de destino. Los

direccionadores (que también son servidores de NHRP) situados en la vía de acceso direccionada comprueban si la dirección del protocolo de destino es una dirección a la que pueden servir.

Si el direccionador puede satisfacer la solicitud, devolverá una Next Hop Resolution Reply (Respuesta de resolución del salto siguiente) con la dirección NBMA de la estación de destino. El originador podrá entonces establecer un circuito virtual directo con el destino. Si no puede satisfacer esta solicitud, el direccionador la reenviará al direccionador del salto siguiente. Este reenvío proseguirá hasta que se satisfaga la solicitud o se determine que no se puede acceder al destino.

Para utilizar terminología de cliente/servidor, un dispositivo puede ser al mismo tiempo cliente y servidor. Cliente es el dispositivo que origina Next Hop Resolution Requests y servidor el que proporciona Next Hop Resolution Replies con información de la dirección NBMA. El 2210 es un dispositivo de este estilo; el cliente se "registra" conceptualmente en la función del servidor en la misma máquina, aunque en realidad no fluye ninguna Registration Requests (Solicitud de registro). El servidor también da soporte a registros NHRP de clientes de NHRP remotos.

La información que proporcionan los clientes a su servidor y los servidores a los peticionarios, debe renovarse periódicamente y puede depurarse si así lo dictan las condiciones. Clientes y servidores mantienen antememorias de información de resolución que han enviado y recibido; se usan períodos de tiempo de retención para asignar una edad a las entradas o ejecutar renovaciones.

Beneficios de la implementación de IBM y NHRP

Por lo general, el uso de atajos de NHRP puede:

- Mejorar el rendimiento de extremo a extremo eliminando saltos entre direccionadores cuando el origen y el destino están en la misma red NBMA y pueden comunicarse directamente.
- Reducir la carga de los direccionadores de red, ya que estos no tratan tráfico que, sin NHRP tendrían que manejar. Esto puede reducir los costos generales ya que son necesarios menos direccionadores o menos anchura de banda.

La implementación ejecutada por IBM de NHRP proporciona los beneficios adicionales siguientes:

- El borrador de NHRP no trata el uso de protocolos en un entorno Emulated LAN. No obstante, la implementación ejecutada por IBM de NHRP incluye consideraciones para tales tipos de entornos; los paquetes de NHRP pueden fluir entre direccionadores sobre conexiones ELAN y pueden establecerse VC de atajo.
- Direccionamiento de un salto: los dispositivos ATM que no dan soporte a NHRP pueden ser el destino de los atajos, eliminando otro salto de direccionador para el tráfico, al ampliar la definición de los dispositivos que reciben "servicios" para incluir atajos que comparten una subred de protocolo con el servidor. Por ejemplo, todas las direcciones IP de una subred classical IP de la cual forma parte un servidor, reciben "servicios" del mencionado servidor. La función NHRP actúa de interfaz con los componentes classical IP 1577 y LAN Emulation para usar las posibilidades de resolución de dirección ATM y aplicarlas a las solicitudes de NHRP. Esta mejora puede incluso usarse para el tráfico con los dispositivos conectados a LAN de legado que se conectan a ATM mediante conmutadores de LAN; el servidor de NHRP en el

direccionador responde al cliente con información de direccionamiento ATM para el conmutador de la LAN, lo que permite al cliente ir directamente por atajo a dicho conmutador. Para consultar ejemplos de estos casos de “direccionamiento de un salto”, consulte la Figura 26 en la página 433 y la Figura 27 en la página 436

Nota: Un salto es una operación efectuada por un direccionador tradicional cuando reenvía paquetes de una subred a otra. En particular, dichas operaciones están (1) efectuando una búsqueda en un identificador de subred de la capa 3 (2) determinando el “salto siguiente” de salida del paquete (3) desmantelando y sustituyendo la cabecera de paquete de la capa 2, eliminando información de enlace de ingreso y añadiendo información de enlace de salida. Por lo tanto, en el caso del direccionamiento de “un salto”, esta operación se produce una vez durante la transferencia de un paquete desde su origen a su destino.

- La implementación de IBM puede funcionar en redes donde algunos direccionadores no den soporte a NHRP. Si el direccionador de salto siguiente no puede dar soporte a NHRP, puede establecerse un VC de atajo hacia el “último” servidor de la vía de acceso. Consulte “atajos de direccionador a direccionador no permitidos” en la página 445 y “Listas de exclusiones” en la página 443.
- El cliente puede configurar el 2210 para que establezca atajos sólo cuando el tráfico a un destino sea superior a un ritmo de datos determinado. Esto puede eliminar la creación de VC para tráfico de bajo volumen o de una vez (por ejemplo, detecciones de condiciones de excepción de SNMP). Consulte el “parámetro data-rate” en la página 457 y el “parámetro attempt shortcuts?” en la página 456.
- El direccionador proporciona soluciones para el efecto “dominó” que se describe en el borrador de NHRP. Consulte el “parámetro attempt shortcuts?” en la página 456.
- Todos los direccionadores conectados a ATM de la vía de acceso direccionada deben dar soporte a NHRP para obtener beneficios óptimos, aunque 2210 puede seguir funcionando y proporcionando atajos en una red mixta.

Características de rendimiento

NHRP se usa durante el contacto inicial de un dispositivo de origen con un destino. Una vez se haya establecido un VC de atajo, NHRP ya no participará en la transferencia real de los datos. Las salvaguardas aseguran que el tráfico NHRP no se vuelva a intentar para cada paquete. Asimismo, la implementación que efectúa IBM proporciona una opción para que los atajos de NHRP sólo se soliciten cuando el tráfico para un destino determinado supere un umbral de velocidad de datos configurable. Esto puede evitar, por ejemplo, el establecimiento de circuitos virtuales que sólo se usen para una trama de detección de condición de excepción SNMP generada por un sistema principal IP.

El funcionamiento de NHRP no influye en el rendimiento de la vía de acceso rápida del direccionador y no influirá significativamente en la vía lenta. Cuando hay atajos disponibles, el rendimiento mejora eliminando los saltos extraños sobre la red ATM. Además, el rendimiento de los direccionadores intermedios eludidos por los atajos de NHRP mejora, ya que estos direccionadores manejan menos tráfico.

Nota: Si una configuración no incluye una interfaz 1577 (es decir, sólo se configura el direccionador para ELAN), sólo podrán establecerse VC de atajo

para el direccionador desde clientes que den soporte a las extensiones de IBM. Esta limitación puede evitarse definiendo simplemente una interfaz 1577 en el direccionador.

Ejemplos de configuraciones de NHRP

Los párrafos siguientes presentan ejemplos de configuraciones de NHRP.

NHRP en un entorno RFC 1577 Classic IP con todos los dispositivos capacitados para NHRP

En esta imagen, los clientes de NHRP usan conexiones RFC 1577 para comunicarse con el direccionador. Usan protocolo NHRP para informarse en el servidor de NHRP sobre sus respectivas direcciones ATM. A continuación, establecer un circuito virtual directo entre sí para el tráfico IP.

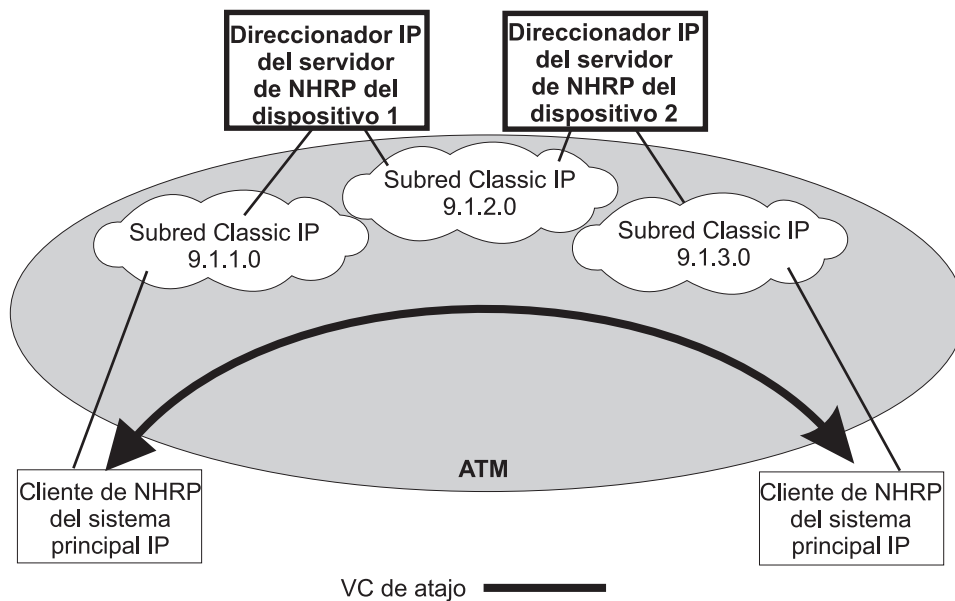


Figura 27. NHRP en un entorno Classic IP

NHRP en un entorno Classic IP con dispositivos no capacitados para NHRP

Este ejemplo muestra cómo puede usarse NHRP entre dos dispositivos 1577 cuando uno de ellos no da soporte a NHRP. En este caso, el dispositivo 2 proporciona al cliente de NHRP la dirección ATM del dispositivo no capacitado para NHRP y el cliente puede establecer un atajo para el tráfico destinado al sistema principal no capacitado para NHRP. No obstante, cuando el tráfico fluye del dispositivo no capacitado para NHRP, lo hace en la vía de acceso direccionada al dispositivo 2; a continuación, este dispositivo actúa como un cliente de NHRP y establece un atajo al destino.

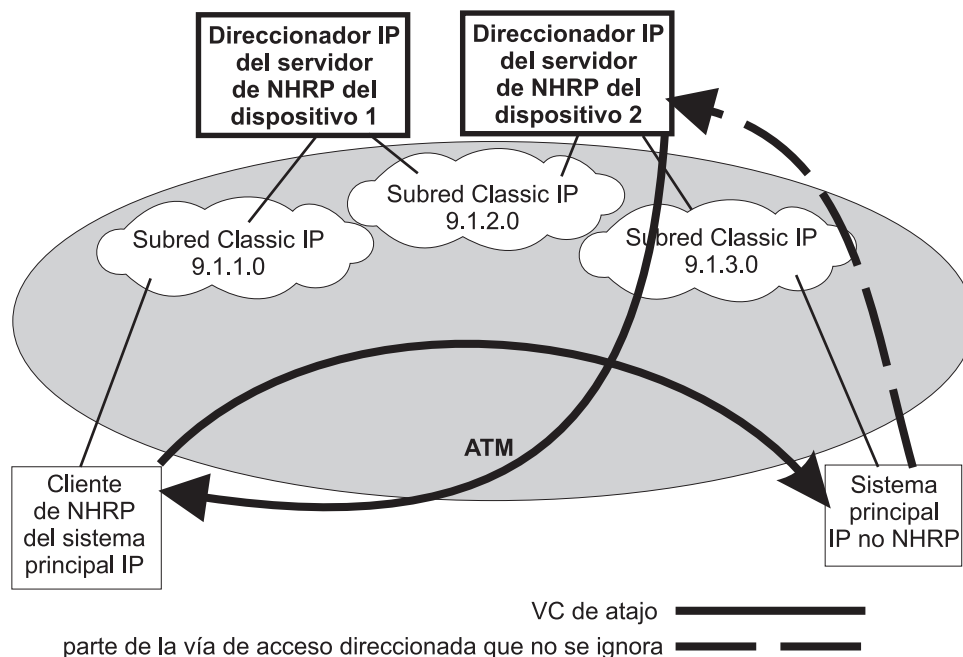


Figura 28. NHRP en un entorno Classic IP con dispositivos no capacitados para NHRP

NHRP en un entorno de LAN Emulation puro

En el caso de la emulación de LAN, los direccionadores usan las extensiones de IBM para proporcionar información de NBMA para dispositivos en las ELAN. Cuando el dispositivo 1 recibe tráfico del sistema principal A destinado al sistema principal B, origina una Next Hop Resolution Request y la envía por la vía de acceso direccionada. El dispositivo 2 responde a la solicitud con información de NBMA sobre el sistema principal B, una de las estaciones a la que sirve ya que están en la misma ELAN. A continuación, el dispositivo 1 establece un VCC directo de datos al sistema principal B incluso aunque éste no participe o dé soporte a los intercambios de NHRP. Tenga en cuenta que este VCC sólo se usará para el tráfico cuya dirección sea de A a B. Asimismo, cuando el sistema principal B envíe tráfico al sistema principal A, el dispositivo 2 generará una Next Hop Resolution Request, el dispositivo 1 responderá con información de direccionamiento sobre el sistema principal A y el dispositivo 2 establecerá un VCC directo de datos a A para el tráfico que vaya de B a A.

Los LEC de este ejemplo son dispositivos que cumplen el estándar sin soporte de NHRP. Deben satisfacer los requisitos de LEC descritos en "Implementación de NHRP" en la página 440.

No debe configurarse nada en especial en estos dispositivos o en los servidores de NHRP. El tráfico de NHRP fluye sobre la subred ELAN sin VC adicionales.

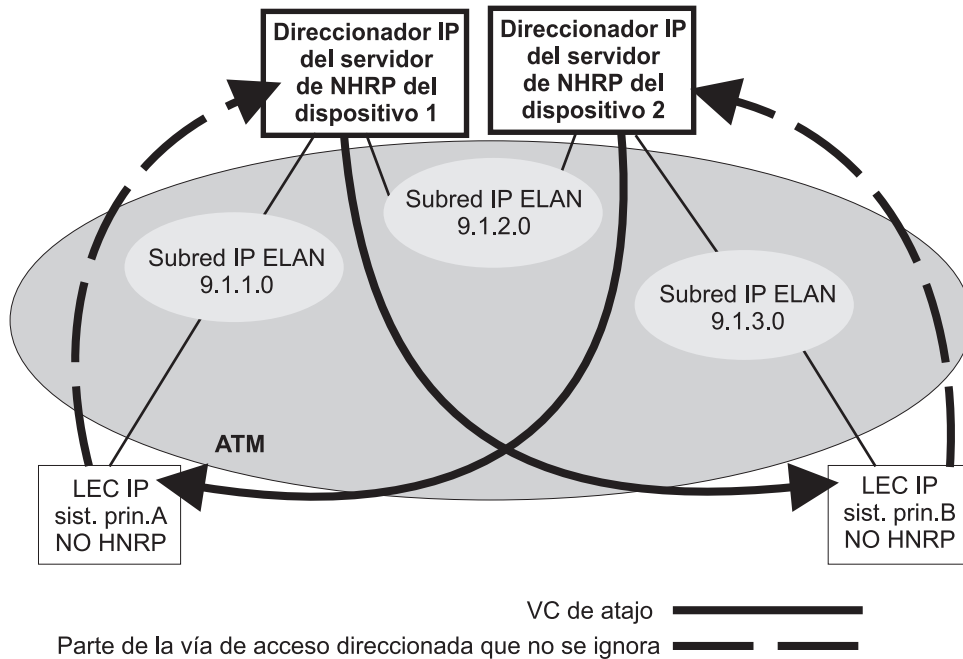


Figura 29. NHRP en un entorno ELAN

NHRP en un entorno de LAN Emulation con conmutadores de LAN

En este ejemplo, las estaciones de origen y de destino están conectadas a LAN legales y no están conectadas a la red ATM. Los conmutadores de LAN que funcionan como clientes de LAN Emulation dan conectividad ATM a los dispositivos LAN legales. Las mejoras efectuadas a NHRP y las extensiones de IBM permiten el mismo tipo de "direccionamiento de un salto" en este entorno que el descrito en el ejemplo anterior. Gracias a las mejoras, los servidores intercambian las direcciones MAC reales y la información de direccionamiento de los dispositivos LAN legales. A continuación, los 2210 pueden establecer VCC directos de datos con los conmutadores y pasar el tráfico directamente. En la vía de acceso sólo hay un "salto" de direccionador, aunque el tráfico pase a través de dos conmutadores de LAN.

Este ejemplo también ilustra que el entorno ELAN puede ser de red en anillo o Ethernet o cualquier mezcla de tipos de LAN.

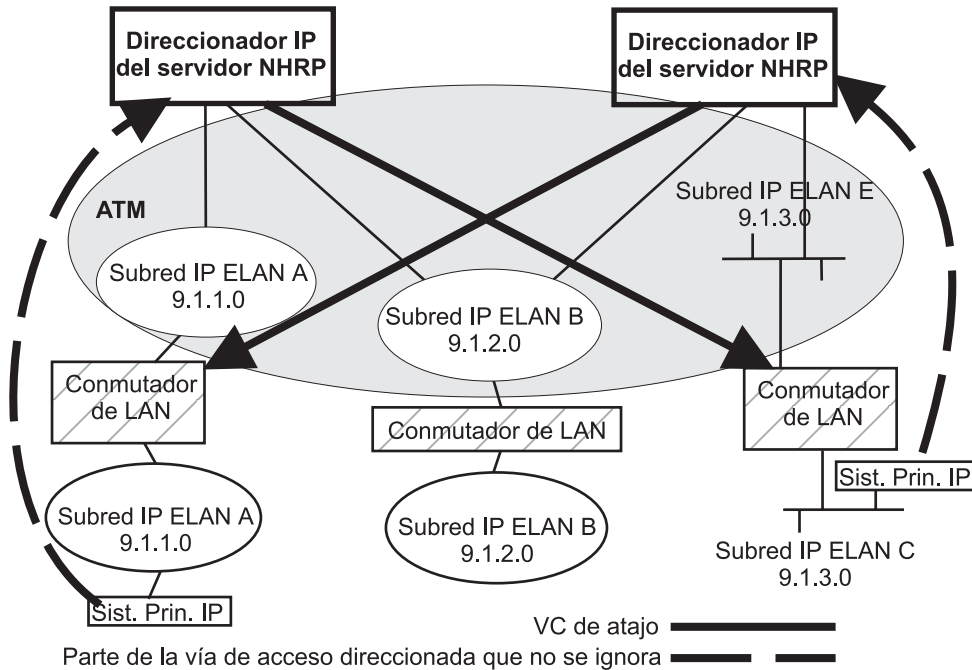


Figura 30. NHRP en un entorno ELAN con conmutadores de LAN

NHRP en un entorno ELAN o classical IP mixto

La función NHRP en el direccionador puede funcionar con interfaces Classic IP y ELAN en la misma red. En este ejemplo, el cliente de NHRP da soporte a las extensiones de IBM y puede atajar directamente al destino LEC en el caso del tráfico que siga dicha dirección.

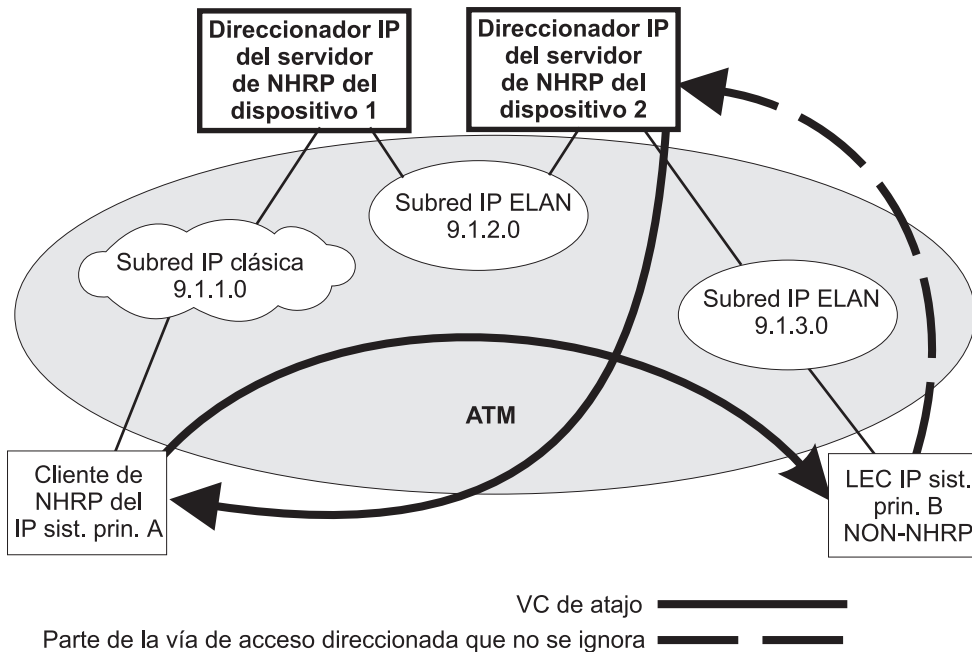


Figura 31. NHRP en un entorno ELAN o classical IP mixto

NHRP a un direccionador de salida

No es necesario que las estaciones de origen o las de destino del tráfico de protocolo pertenezcan a subredes servidas por participantes de NHRP. Pueden acceder a la red ATM a través de direccionadores que se comuniquen con los dispositivos NHRP. En dicho caso, 2210 proporciona atajos a través de la red ATM para eliminar la mayor cantidad posible de saltos.

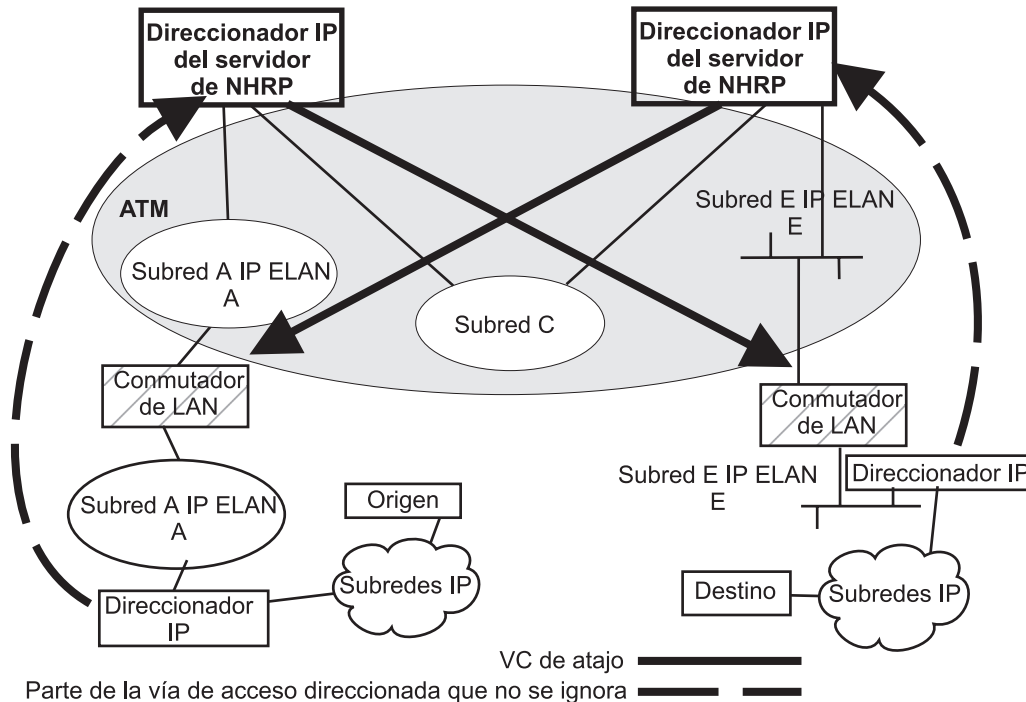


Figura 32. NHRP a un direccionador de salida

Implementación de NHRP

NHRP interactúa con la función de direccionador del direccionador. Cuando esta función está reenviando paquetes por la vía de acceso direccionada y NHRP obtiene satisfactoriamente un VC de atajo, NHRP actualizará la función de direccionador para enviar el paquete directamente por el VC de atajo.

NHRP actualiza la tabla de reenvíos de la función de direccionamiento después de que se active el VC. Esto permite que se produzca la conmutación de la vía de acceso direccionada a la vía de acceso de atajo, sin que se produzcan pérdidas de paquetes.

Cuando se usa un atajo de NHRP, el direccionador transmite tramas a una dirección de salto siguiente de una subred a la que el mismo direccionador no pertenece. Por ello, el NET o interfaz que proporciona la vía de acceso de salida al tráfico se llama "virtual" network interfaz (interfaz de red virtual).

Virtual Network Interface (VNI)

Por lo general, el flujo de paquetes de salida de un direccionador tiene las restricciones siguientes:

- Incapacidad de enviar paquetes directamente a direcciones de red que no estén definidas en una interfaz de red.
- Incapacidad de enviar paquetes a tipos de red (por ejemplo, ELAN de red en anillo) a menos que dicho tipo de red esté definido en una interfaz de red.

El manejador de red Virtual Network Interface (VNI) elimina estas restricciones, lo que permite al direccionador reenviar paquetes directamente a saltos siguientes obtenidos a través de NHRP (rutas atajo). Permite el direccionamiento de un salto, en el que las rutas de atajo de NHRP pueden establecerse directamente con dispositivos que no dan soporte a NHRP.

VNI da soporte a interfaces de red de redes en anillo, Ethernet V2 y Ethernet DIX ELAN e interfaces de red classic IP. Cuando la vía de acceso de salida va a usar una interfaz classic IP (1577), la implementación utilizará, en realidad, la interfaz del manejador de red 1577 para VNI existente. No obstante, cuando esta vía de acceso deba utilizar un atajo LANE, accederá a una interfaz única. Esto recibe el nombre de Interfaz de atajos LANE (LSI). LSI es diferente de la interfaz LEC tradicional ya que proporciona más de un tipo de encapsulación de LAN; es decir, puede establecerse un VC usando la encapsulación de red en anillo mientras que otro usa Ethernet V2. Además, LSI proporciona conexiones a más de una Emulated LAN, mientras que una interfaz LEC tradicional se conecta únicamente con una ELAN.

Cuando habilita NHRP, se crea una LSI por cada adaptador ATM. A esta LSI se le asigna el número de interfaz disponible siguiente y se listará cuando invoque funciones de consola que muestren información sobre las interfaces del direccionador.

Interfaz de atajos LANE (LSI)

Los atajos LANE proporcionados por las extensiones IBM a NHRP no son compatibles con algunas implementaciones en pila de protocolos de estación final y de LAN Emulation Client (LEC). En esta sección describimos cómo pueden surgir estas incompatibilidades y, en algunos casos, cómo pueden superarse usando opciones de configuración.

Los LEC paranoides son dispositivos que usan el LAN Emulation Flush Protocol para verificar que los clientes que establezcan VCC directos de datos con ellos sean miembros de su ELAN. Estos dispositivos no funcionarán con atajos NHRP generados por LSI dado que la LSI no forma parte del ELAN de destino.

Nota: La opción de configuración “Exclude List” (lista de exclusiones) puede usarse para evitar atajos a LEC paranoides, tal como se describe en “Listas de exclusiones” en la página 443.

Por omisión, la LSI usará la dirección del MAC incorporada en el adaptador ATM asociado como dirección del MAC de origen de las tramas transmitidas por los VCC de atajo LANE. Es posible, aunque poco probable, que esto pueda confundir a alguna implementación en pila de protocolo de estación final, ya que la dirección del MAC no coincidirá con la del direccionador que use la estación final como pasarela para transmitir paquetes a la dirección IP asociada.

Para que ello ocurra, la estación final debería informarse de las direcciones del MAC del direccionador en tramas IP de una difusión individual, lo que no es normal (por lo general, las correlaciones de IP a MAC se saben a partir de paquetes ARP). No obstante, si esto se produce, la estación final puede usar la dirección del MAC obtenida como dirección del MAC de destino de las tramas que transmite al destino IP asociado en vez de usar la dirección del MAC del direccionador. Tales tramas se eliminan o bien se reenvían sobre VCC de métodos abreviado LANE. El reenvío sólo se produce si el LEC se entera de la vinculación de la dirección MAC a ATM en las tramas recibidas (lo cual es una elección de implementación opcional).

En ambos casos, las tramas no llegarán a destino ya que la LSI descarta las tramas recibidas en un VCC de atajo LANE. Además, la LSI libera el VCC de atajo LANE y no se establecerán más atajos con la dirección ATM asociada. A partir de ese momento, el tráfico para los destinos asociados con la dirección ATM seguirá la vía de acceso direccionada. Tenga en cuenta que los mensajes ELS y la visualización de consola de los atajos LANE ayudan a identificar estos destinos.

Puede configurarse la LSI para que no use la dirección del MAC administrada universalmente como dirección del MAC de origen. Con esta opción, tiene dos posibilidades de elección para la dirección del MAC de origen:

1. Puede usar la dirección del MAC del direccionador del último salto, proporcionada en el paquete de respuesta de resolución de NHRP, como la dirección del MAC de origen.

El uso de la dirección del MAC del direccionador del último salto como dirección del MAC de origen resuelve el problema de la confusión de apilamiento del protocolo de la estación final pero introduce otro problema potencial. Puede provocar confusión en los LEC que se enteren de la vinculación de la dirección del MAC a ATM a partir de las tramas recibidas y, por consiguiente, no debe usarse con LEC que tengan este tipo de aprendizaje. Por ejemplo, el LEC del puente 8281 ATM-LAN de IBM tiene este tipo de aprendizaje.

2. Puede configurar la dirección del MAC de origen.

Esta dirección puede configurarse para evitar el problema de las direcciones del MAC duplicadas observado en una ELAN, que se produce debido a atajos entre ELAN. La dirección del MAC debe configurarse para esta red LSI cuando hay entradas de atajos LANE no permitidas. Consulte "Métodos abreviados LANE" en la página 463 para obtener detalles sobre cómo visualizar entradas de atajos LANE no permitidas.

Estas opciones de configuración se proporcionan para maximizar la flexibilidad en la consecución de compatibilidad con el mayor conjunto posible de destinos en una instalación determinada. Consulte "Configuración de la interfaz de atajos LANE (LSI)" en la página 447 para obtener información detallada y "Change" en la página 454 para obtener una descripción del mandato **change**.

Parámetros de configuración

Esta sección describe algunos parámetros de configuración relacionados con NHRP y el uso que se recomienda. Consulte "Mandatos de configuración de NHRP" en la página 449 para obtener información sobre la sintaxis del mandato, sus parámetros, los valores válidos y los valores por omisión.

Configuración automática de NHRP

NHRP se habilita por omisión si IP está presente en la entrega. Puede inhabilitarse entrando el mandato **disable NHRP** desde el indicador `NHRP config>`. Consulte “Acceso al proceso de configuración de NHRP” en la página 449 para obtener información adicional.

Cuando use un archivo de configuración existente, NHRP se habilitará por omisión si no se configuró previamente. El archivo de configuración se actualizará automáticamente en el momento de ejecución para crear interfaces de atajos de NHRP. Deberá guardar este archivo de configuración actualizado y reiniciar el sistema para que el cliente de NHRP use los atajos LANE.

Listas de exclusiones

La configuración le permite crear una lista de direcciones de protocolo (y máscaras asociadas) que representan dos tipos de dispositivos:

- Direccionadores de salto siguiente que no contienen una función de servidor de NHRP
- Dispositivos de destino a los que no deben permitirse los VC de atajo

Direccionadores del salto siguiente: La lista de exclusiones puede usarse para identificar direccionadores que estén en la vía de acceso direccionada pero que no den soporte a la función de servidor de NHRP.

El servidor responde a una Next Hop Resolution Request proporcionando la dirección ATM del direccionador del salto siguiente cuando todo lo indicado a continuación sea verdadero:

- La dirección del salto siguiente es diferente de la dirección de destino.
- La interfaz del direccionador con el direccionador del salto siguiente es una ATM classical IP o una subred ELAN.
- La dirección del salto siguiente está en la lista de exclusiones.

Al procesar la solicitud, el direccionador no reenvía la Resolution Request a la dirección del salto siguiente, pero responde al cliente con información de direccionamiento que permite a éste establecer un VC de atajo al direccionador del salto siguiente.

Nota: Si el direccionador del salto siguiente es uno de los Disallowed R2R Shortcuts (atajos R2R no permitidos), el direccionador enviará un NAK a la Resolution Request en vez de una respuesta positiva.

Por lo general, si el direccionador del salto siguiente está en la lista de exclusiones, no deberá enviar ningún paquete NHRP que sólo manejaría un servidor de NHRP.

Dispositivos de destino: La lista de exclusiones también puede usarse para evitar VC de atajos a una dirección de protocolo determinada (por ejemplo, un dispositivo de una subred ELAN o CIP que sólo pueda dar soporte a un número pequeño de VC).

Al procesar una Next Hop Resolution Request para un dispositivo de destino, el servidor responde al cliente con información de direccionamiento que permite a

éste establecer un VC de atajo al mismo direccionador, cuando el resto de lo que indicamos a continuación es verdad:

- La dirección del salto siguiente es la misma que la dirección de destino.
- La interfaz del direccionador con el destino es una ATM classical IP o una subred ELAN.
- La dirección de destino está en la lista de exclusiones.

Extensiones

El protocolo NHRP incluye **Extensions** (extensiones). Las extensiones se añaden a paquetes NHRP. Se usan para solicitar funciones adicionales a participantes de NHRP. El uso del parámetro **extensions** le permite determinar si el direccionador envía algunas extensiones:

- extensiones de información de la vía de acceso
- extensiones IBM privadas del proveedor

Extensiones de información de la vía de acceso: Hay tres extensiones definidas en NHRP para proporcionar información de vía de acceso. Estas extensiones pueden usarse para ayudar a supervisar la misma solicitud, determinar la vía de acceso seguida por ésta, determinar quién generó la respuesta y la vía de acceso que siguió ésta. Las extensiones de información de la vía de acceso son:

- Forward Transmit - (Transmisión de reenvío) Cada servidor del salto siguiente (NHS) que reenvía la solicitud a lo largo del recorrido debe añadir información sobre sí mismo.
- Responder Address - (Dirección del emisor de la respuesta) El servidor del salto siguiente (NHS) que genera la respuesta debe añadir información sobre sí mismo.
- Reverse Transmit - (Transmisión inversa) Cada servidor del salto siguiente (NHS) que reenvía la respuesta a lo largo del recorrido debe añadir información sobre sí mismo.

Puede configurarse el direccionador para que envíe una de estas extensiones o todas en los paquetes Next Hop Resolution Request que genere. La información recibida en los paquetes de respuesta se visualizará en los mensajes NHRP ELS del direccionador.

Extensiones IBM privadas del proveedor: Para dar soporte a NHRP en un entorno Emulated LAN, el servidor añade extensiones únicas del proveedor a paquetes de NHRP. Estas extensiones actúan como “consultas”; el cliente de NHRP las pone en la Next Hop Resolution Request. Si el servidor da soporte a esta función, responderá con tres extensiones correspondientes que contengan la información de dirección ELAN (dirección del MAC, dirección ATM e información de direccionamiento); estas extensiones se incluyen en la Next Hop Resolution Reply.

Puede configurarse el direccionador para que no dé soporte a las extensiones específicas de IBM. Si estas extensiones no se usan, no serán posibles los atajos directos a dispositivos de ELAN. Use la opción “Exclude List” para inhabilitar selectivamente atajos a algunos dispositivos ELAN.

atajos de direccionador a direccionador no permitidos

El funcionamiento de NHRP puede producir el establecimiento de vías de acceso de tránsito a través de red NBMA entre direccionadores. No obstante, el establecimiento de un atajo NHRP que atravesase un límite donde la información usada en la selección de rutas se pierde, puede producir un bucle de direccionamiento. Tales situaciones incluyen la pérdida de información de vector de vía de acceso BGP y el interfuncionamiento de protocolos de direccionamiento múltiple con métricas disimilares. En tales circunstancias, los atajos NHRP entre direccionadores no deben permitirse. Esta situación puede evitarse si no hay vías de acceso “back door” (traseras) entre la entrada y el direccionador de salida fuera de la red NBMA.

El servidor permite atajos de direccionador a direccionador (R2R) por omisión. No obstante, al configurar atajos R2R no permitidos, puede crear una lista de direcciones de destino o de direccionador para la que el direccionador no permita atajos.

Para crear un atajo R2R no permitido, debe especificar una dirección de protocolo y una máscara. La dirección de protocolo es el destino o un direccionador y la máscara permite un rango de direcciones.

Para ilustrar cómo especificar atajos R2R no permitidos usando direcciones de protocolo y máscaras, observe el diagrama de red siguiente:

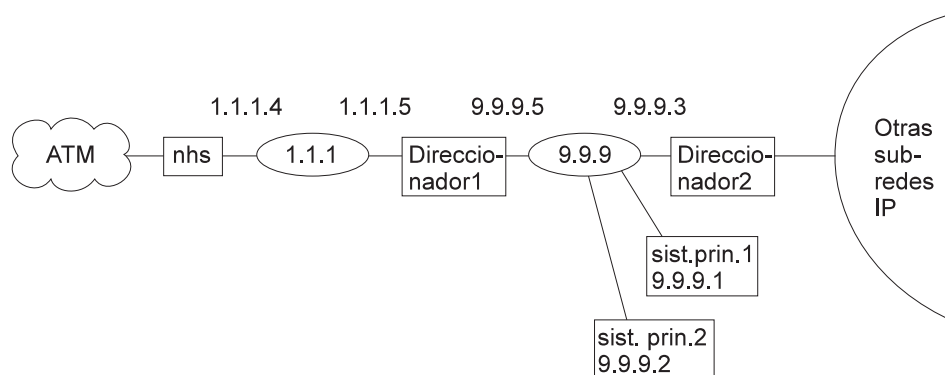


Figura 33. Uso de atajos de direccionador a direccionador no permitidos

Ejemplo 1: Una entrada que tenga la *dirección=9.9.9.1* *máscara=255.255.255.255* provocaría que el NHS enviase un NAK al remitente de una Next Hop Resolution Request con la dirección del protocolo de destino 9.9.9.1 (HOST1). Dado que 9.9.9.1 no está conectada directamente a una de las subredes de dispositivo, pero se puede acceder a ella mediante otro direccionador, el direccionador comprobará la lista de atajos R2R no permitidos.

Ejemplo 2: Una entrada con *dirección=9.9.9.0* *máscara=255.255.255.0* provocará que el direccionador envíe un NAK a todas las direcciones de destino entre 9.9.9.1 y 9.9.9.255. No será posible acceder a Sist.princ.1, Sist.princ.2 y Direccionador2 usando atajos al direccionador pero sí que será posible acceder a dispositivos situados en otras subredes servidas por Direccionador2.

Ejemplo 3: Una entrada con *dirección=1.1.1.5* *máscara=255.255.255.255* provocará que el direccionador responda negativamente a cualquier destino cuyo

direccionador de salto siguiente sea 1.1.1.5, Direccionador1. El direccionador responderá negativamente a cualquier dirección de la subred 9.9.9 y a cualquier dirección de las otras subredes IP a las que se acceda a través del direccionador 9.9.9.3 ya que el salto siguiente es 1.1.1.5.

Ejemplo 4: Una entrada con *dirección=cualquier máscara=0.0.0.0* inhabilitará los atajos R2R para todas las direcciones.

Uso del control de acceso de protocolos

Este parámetro determina si los controles de acceso a la capa de protocolo se comprobarán y, si se comprueban, cómo se aplicarán los controles a los paquetes NHRP.

Si este parámetro de configuración se establece en el valor por omisión *none* (ninguno), los controles de acceso de la capa de protocolo no se comprobarán.

Con el valor *source and destination* (origen y destino), cuando el peticionario de NHRP no sea un direccionador, se asumirá que la dirección IP del cliente de NHRP es el origen de todos los paquetes IP que transmitirá el cliente usando la ruta de atajo NHRP. El direccionador negará solicitudes de atajo NHRP a los clientes de NHRP que no sean direccionadores si se están filtrando paquetes IP para el par de direcciones origen/destino IP, en la que el origen es la dirección del cliente de NHRP.

Si selecciona la opción *destination only* (sólo destino) el direccionador negará solicitudes de atajo a cualquier cliente de NHRP si se están filtrando paquetes IP a la dirección de destino. Si los clientes de NHRP no son fiables, deberá seleccionarse *destination only*. *destination only* puede ser la mejor opción cuando los clientes de NHRP no son direccionadores y tienen varias direcciones IP o son clientes que no son direccionadores y que transmiten paquetes que provienen de otros orígenes.

Los clientes de NHRP que residen en los direccionadores usan las rutas de atajo NHRP para reenviar paquetes de otros orígenes: por consiguiente, si *source and destination* está configurado y el direccionador recibe una solicitud de atajo de otro direccionador, el direccionador aplicará los filtros IP igual que cuando se selecciona *destination only*.

Controles de acceso NHRP

Los controles de acceso de NHRP para denegar atajos a algunas direcciones IP pueden definirse añadiendo estas direcciones a la lista de exclusiones y los atajos de direccionador a direccionador no permitidos.

ID de la red ATM

Dado que un servidor puede tener más de un adaptador ATM, puede estar conectado a dos redes diferentes o no asociadas. Debe tenerse en cuenta esta posibilidad al decidir cuándo deben permitirse VC de atajo.

Puede determinarse qué interfaces deben tratarse como si estuvieran conectadas a la misma red ATM física asignando a cada interfaz ATM un ID de red usando el mandato **set** en el indicador ATM Interface Config>, tal como se describe en el capítulo "Using and Configuring ATM" (Uso y configuración de ATM) en el manual *Guía del usuario de software*

Se considera que las interfaces ATM que tienen el mismo ID de red pertenecen a la misma red. Por omisión, se asigna a todas las interfaces ATM el ID de red 0.

Configuración de la interfaz de atajos LANE (LSI)

La interfaz de atajos LANE (LSI) de NHRP se crea automáticamente para cada adaptador ATM cuando se habilita NHRP para el direccionador. LSI usa valores por omisión para los parámetros siguientes.

- ESI
- Selector
- Use Best Effort Service for Data VCCs
- Peak Cell Rate of outbound Data VCCs
- Sustained Cell Rate of outbound VCCs
- Use ATM adapter's universally administered MAC address for source

Los valores por omisión pueden modificarse usando el mandato **change** en el indicador NHRP Advanced config>. Consulte "Change" en la página 454.

Configuración de dispositivos en una red ATM

Si tiene un cliente/servidor de NHRP y su configuración necesita que dé una dirección ATM del servidor de NHRP del direccionador, deberá seleccionar la dirección ATM adecuada. Deberá usar una dirección asociada a una "interfaz ATM" en el dispositivo y deberá asignar una dirección IP a esta interfaz. Los dos últimos dígitos de la dirección ATM del direccionador, el selector, se asignan dinámicamente después de activar el direccionador (y pueden cambiar si la configuración del direccionador cambia), a menos que haya configurado un selector específico.

Puede especificar la dirección ATM, incluyendo el selector, entrando **prot arp** en el indicador talk 6 Config>, seguido de **add atm**, que da la dirección IP deseada, y especificando un selector. Es el mismo procedimiento que el usado para definir un cliente de ATMARP.

Uso de NHRP con LAN Emulation

Si desea usar NHRP en el dispositivo, deberá configurar todos los LEC con una dirección del MAC exclusiva administrada localmente (LAA). Si no configura los LEC con una LAA exclusiva, la función de atajo de NHRP al conmutador o dispositivo correspondiente no funcionará porque:

- El tráfico enviado en un VCC de atajo NHRP LANE contendrá la dirección del MAC Universally Administered (universalmente administrado) como la dirección del MAC de origen.
- Algunos dispositivos de red tendrán conocimiento de la asociación entre la dirección del MAC y el VCC a partir del tráfico que haya recibido el dispositivo. Estos dispositivos usarán el NHRP VCC para transmitir datos.
- Si el direccionador detecta tráfico de entrada en un NHRP VCC, asumirá que se ha producido un estado de error y cerrará el VCC, y evitará nuevos atajos al dispositivo de red.

Nota: Por omisión, el direccionador habilita las LAN Emulation Extensions (extensiones LAN Emulation) en NHRP, por lo que deberá inhabilitar las extensiones o configurar la dirección del MAC administrada localmente única para cada LEC.

Configuración y supervisión de NHRP

Este capítulo describe cómo configurar y supervisar Next Hop Resolution Protocol (NHRP). Para obtener una descripción de este protocolo, Consulte “Visión general de Next Hop Resolution Protocol (NHRP)” en la página 433.

Este capítulo contiene las secciones siguientes:

- “Acceso al proceso de configuración de NHRP”
- “Mandatos de configuración de NHRP”
- “Acceso al proceso de supervisión de NHRP” en la página 460
- “Mandatos de supervisión de NHRP” en la página 460
- “Rastreo de paquetes de NHRP” en la página 466
- “NHRP Soporte de reconfiguración dinámica del servidor NHRP” en la página 467

Acceso al proceso de configuración de NHRP

Para acceder a la configuración de NHRP:

1. En el indicador de supervisión del operador (*), escriba **talk 6** y pulse Intro.
2. En el indicador `config>`, escriba **protocol nhrp** y pulse Intro.
3. Aparecerá el indicador `NHRP config>`.

Mandatos de configuración de NHRP

Esta sección explica todos los mandatos de configuración de NHRP, tal como se muestra en la Tabla 109. Entre los mandatos en el indicador `NHRP config>`.

Tabla 109. Resumen de mandatos de configuración de NHRP

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte la sección “Cómo obtener ayuda” en la página xxix.
Enable NHRP	Activa NHRP para todas las interfaces que no estén definidas explícitamente.
Disable NHRP	Desactiva NHRP para todas las interfaces que no estén definidas explícitamente.
List	Muestra la configuración de NHRP.
Advanced config	Le lleva al indicador <code>NHRP Advanced config></code> , en el que podrá entrar otros mandatos como los descritos en “Mandatos de configuración avanzada de NHRP” en la página 451.
Exit	Le devuelve al nivel de mandatos anterior. Consulte la sección “Cómo salir de un entorno de nivel inferior” en la página xxix.

Mandatos de configuración de NHRP (Talk 6)

Enable NHRP

Use el mandato `enable` para habilitar NHRP en todas las interfaces que no estén definidas explícitamente usando un mandato de configuración avanzada de NHRP. Se trata de una forma simple de activar y ejecutar NHRP con parámetros por omisión.

Sintaxis:

```
enable          nhrp
```

Disable NHRP

Use el mandato `disable` para inhabilitar NHRP en todas las interfaces que no estén explícitamente definidas con un mandato de configuración avanzada de NHRP.

Sintaxis:

```
disable          nhrp
```

Ejemplo:

```
NHRP config> disable  
  Disable NHRP for the router [No]:
```

Advanced Config

Use el mandato `advanced` para ir al indicador de configuración avanzada de NHRP, `NHRP Advanced config>`. Desde este indicador, podrá entrar los mandatos descritos en “Mandatos de configuración avanzada de NHRP” en la página 451.

Sintaxis:

```
advanced          nhrp
```

Ejemplo:

```
NHRP config> advanced  
  NHRP Advanced config>
```

Nota: La mayoría de las instalaciones no necesitarán usar el mandato “advanced”. El mandato `enable NHRP` es suficiente para habilitar NHRP con opciones por omisión recomendadas.

List

Use el mandato `list` para hacer una lista de la configuración de NHRP.

Sintaxis:

```
list
```

Ejemplo:

Mandatos de configuración avanzada de NHRP (Talk 6)

```
NHRP config> list
Box level NHRP enabled
  Explicit interface definitions override box level setting

Interfaces explicitly defined for NHRP
-----
Interface 0: ATM
  NHRP enabled

NHRP LANE Shortcut Interface:
-----
Interface: 1  ESI: burned-in      Sel: auto
Use Best Effort: no  (Data)
Cell Rate(kbps):  Peak: 155000   Sustained: 155000
ATM adapter's burned-in MAC address is used as source address

General Parameters
-----
Holding time:                20 minutes
Protocol Access Controls:    Use source and destination  address
When should NHC attempt shortcuts?:  Based on datarate
  Data-rate threshold:        10 packets/second
NHS allows shortcuts to ATMARP clients?: Yes

Cache
Sizes
-----
Resolution cache:            10000 entries
Server purge cache:          10000 entries
Server registrations cache:  10000 entries

Extension Usage
-----
Use NHRP Forward transit NHS record client extension: No
Use NHRP Reverse transit NHS record client extension: No
Use Responder Address client extension:                No
Use LANE shortcuts extension:                          Yes

List of NHRP IP exclude records
-----
# Address      Mask
1 6.6.6.6      255.255.255.255
2 5.5.5.0      255.255.255.0

Disallowed router-to-router shortcuts for IP
-----
None
```

Mandatos de configuración avanzada de NHRP

Esta sección explica todos los mandatos de configuración avanzada de NHRP, tal como se muestra en la Tabla 110. Entre los mandatos desde el indicador NHRP Advanced config>.

Tabla 110 (Página 1 de 2). Resumen de los mandatos de configuración avanzada de NHRP

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte la sección “Cómo obtener ayuda” en la página xxix.
Add	Añade una interfaz de NHRP, una lista de exclusiones o métodos abreviados R2R no permitidos.

Mandatos de configuración avanzada de NHRP (Talk 6)

Tabla 110 (Página 2 de 2). Resumen de los mandatos de configuración avanzada de NHRP	
Mandato	Función
Change	Cambia una interfaz de NHRP o cambia una definición de la interfaz de atajo LANE.
Delete	Suprime una interfaz de NHRP, una lista de exclusiones o métodos abreviados R2R no permitidos.
List	Muestra la configuración de NHRP.
Set	Establece parámetros de NHRP.
Exit	Le devuelve al nivel de mandatos anterior. Consulte la sección “Cómo salir de un entorno de nivel inferior” en la página xxix.

Add

Use el mandato **add** para añadir una definición de interfaz explícita, una entrada de la lista de exclusiones o métodos abreviados de direccionador a direccionador no permitidos.

Sintaxis:

add interface definition
 exclude list
 disallowed router-to-router shortcuts

interface definition

Añade una definición de interfaz explícita para habilitar o inhabilitar una interfaz de NHRP. Si NHRP está inhabilitado en una interfaz de red determinada, los paquetes de NHRP no se reenviarán a ningún direccionador al que se acceda a través de dicha interfaz. Además, las tramas de NHRP de entrada se descartarán.

Nota: Cualquier definición de interfaz explícita altera temporalmente el valor de nivel de entrega “NHRP enabled/disabled” (NHRP habilitado/inhabilitado).

Ejemplo: **add int**

```
Interface Number [0]?  
Enable NHRP [Yes]:
```

exclude list

Añade una entrada en la lista de exclusiones. Especifica una dirección de protocolo que deberá excluirse de la red NHRP. Esta opción añade una entrada a la lista de exclusiones y le solicita que añada esta entrada a los métodos abreviados de direccionador a direccionador no permitidos. Consulte “Controles de acceso NHRP” en la página 446 para obtener más información.

Valores válidos: Máscara y dirección IP.

Valor por omisión: Empty (vacío).

Ejemplo: **add exc**

Mandatos de configuración avanzada de NHRP (Talk 6)

```
IP Address [0.0.0.0]? 6.6.6.5
Address Mask [255.255.255.255]?
Deny Shortcuts[Yes]?
Record added to Disallowed Router-to-Router Shortcuts
Record added to Exclude List
```

disallowed router-to-router shortcuts

Añade una dirección de protocolo de direccionador para la que no están permitidos los métodos abreviados.

Consulte “atajos de direccionador a direccionador no permitidos” en la página 445 para obtener más información.

Ejemplo: add dis

```
IP ADDRESS [0.0.0.0]? 8.8.8.1
Address Mask [255.255.255.255]?
```

Valores válidos: Máscara y dirección IP.

Valor por omisión: Empty (vacío).

Delete

Use el mandato **delete** para suprimir una definición de interfaz para NHRP, una entrada de la lista de exclusiones o métodos abreviados de direccionador a direccionador no permitidos.

Sintaxis:

```
delete          interface definition for NHRP
                  exclude list
                  disallowed router-to-router shortcuts
```

interface definition for NHRP

Suprime una definición de interfaz de NHRP explícita.

Ejemplo: del int

```
Interface Number [0]?
```

exclude list

Suprime una entrada de la lista de exclusiones. Esta opción suprime una entrada de la lista de exclusiones y le solicita que suprima esta entrada de los métodos abreviados de direccionador a direccionador no permitidos. Consulte “Controles de acceso NHRP” en la página 446 para obtener más información.

Debe especificar un índice que debe suprimirse. Use el mandato **list exclude** para determinar el índice correcto.

Ejemplo: del exc

```
Enter index of access control to be deleted [1]?
# Address      Mask
1 6.6.6.6      255.255.255.255
Are you sure this the record you want to delete [Yes]?
Record deleted from Exclude List
Delete from Disallowed Router-to-Router Shortcuts [Yes]?
Record deleted from Disallowed Router-to-Router Shortcuts
```

disallowed router-to-router shortcuts

Suprime una entrada de métodos abreviados de direccionador a direccionador no permitidos. Debe especificar un índice que debe suprimirse. Use el mandato **list disallowed** para determinar el índice correcto.

Ejemplo: del dis

```
Disallowed shortcuts index [1]?
```

Change

Use el mandato **change** para modificar definiciones de interfaz de NHRP.

Sintaxis:

```
change          interface definition  
                  nhrp lane shortcut interface
```

interface definition for NHRP

Cambia una definición de interfaz explícita para habilitar o inhabilitar una interfaz de NHRP.

Ejemplo: ch int

```
Interface Number [0]?  
Enable NHRP [Yes]:
```

NHRP LANE shortcut Interface

Cambia una definición de una interfaz de atajo LANE.

Ejemplo: ch nhrp

```
Interface Number of NHRP LANE Shortcut Interface [0]?  
( 1) Use burned in ESI  
Select ESI [1]?  
Use internally assigned selector? [Yes]:  
Use Best Effort Service for Data VCCs? [Yes]:  
Peak Cell Rate of outbound Data VCCs (Kbps) [0]?  
Sustained Cell Rate of outbound Data VCCs (Kbps) [0]?  
Use ATM adapter's burned-in MAC address for source?
```

Interface Number of NHRP LANE Shortcut Interface

Use el número de interfaz asignado al LSI. El número de interfaz puede determinarse usando el mandato **list interface**.

(1) Use burned in ESI

Use el ESI administrado universalmente como parte de la dirección ATM. Es posible que, según la configuración, se le ofrezcan otras opciones.

Select ESI

Especifique el ESI.

Use internally assigned selector

Use el selector asignado internamente o asigne un selector que esté dentro del rango incluido entre 00 y FF.

Use Best Effort Service for Data VCCs

Especifica el tipo de características de tráfico que se asociarán con los VCC de datos. La anchura de banda no se reserva al tráfico de mejor esfuerzo.

Peak Cell Rate of outbound Data VCCs (kbps)

Especifica el tráfico de velocidad mayor de célula (PCR) para los VCC de datos.

Sustained Cell Rate of outbound Data VCCs (Kbps)

Especifica el parámetro de la velocidad sostenida de célula (SCR) para los VCC de datos.

Use ATM adapter's burned-in MAC address for source?

Puede usar como dirección del MAC de origen para métodos abreviados LANE:

1. La dirección del MAC administrada universalmente del adaptador
2. La dirección del MAC suministrada en la respuesta de resolución de NHRP
3. La dirección del MAC que configuró especificando una dirección del MAC con el mandato **change nhrp**.

Consulte "ATM and LAN Emulation" en el manual *Guía del usuario de software* para obtener mayor información.

Nota: Se recomienda que use los valores por omisión hasta que haya determinado las opciones de proceso específicas del entorno.

List

Use el mandato **list** para visualizar información de configuración de NHRP.

Sintaxis:

list all
 exclude list
 disallowed router-to-router shortcuts
 interface definitions
 cache size

all Muestra toda la configuración de NHRP.

Ejemplo: 1 i a11

La salida es la misma que la que se obtiene con el mandato **list**. Consulte "List" en la página 450.

exclude list

Muestra las entradas de la lista de exclusiones.

Ejemplo: 1 i exc

```
List of NHRP IP exclude records
-----
# Address      Mask
1 7.7.7.7      255.255.255.255
```

disallowed router-to-router shortcuts

Muestra los métodos abreviados de direccionador a direccionador no permitidos.

Ejemplo: 1 i dis

```
Disallowed router-to-router shortcuts for IP
-----
1 8.8.8.1      255.255.255.255
2 6.6.6.1      255.255.255.255
```

interface definitions

Muestra las definiciones de interfaces de NHRP.

Ejemplo: 1 i int

Mandatos de configuración avanzada de NHRP (Talk 6)

```
Interfaces explicitly defined for NHRP
-----
None

NHRP LANE Shortcut Interface:
-----
Interface: 3 ESI: burned-in Sel: auto
Use Best Effort: yes (Data)
Cell Rate(kbps): Peak: 0/ 0 Sustained: 1000/538764944
MAC address supplied by NHS is used as source address
```

cache size

Muestra los tamaños de las antememorias.

Ejemplo: `show ip nhrp`

```
Cache
-----
Sizes
-----
Resolution cache: 10000 entries
Server purge cache: 10000 entries
Server registrations cache: 10000 entries
```

Set

Use el mandato **set** para:

Sintaxis:

```
set protocol access control usage
atttempt shortcuts
holding time
data-rate threshold
extensions ...
cache size ...
shortcuts to atmarp clients
```

protocol access control usage

Determina si los controles de acceso de IP se comprobarán y, si es así, cómo se aplicarán a los paquetes NHRP. Consulte “Uso del control de acceso de protocolos” en la página 446 para obtener más información.

Ejemplo: `set prot`

```
Use (Destination, Source & Destination, None) [None]?
```

Valores válidos: None (Ninguno), Source and Destination (Origen y destino), Destination (Destino)

Valor por omisión: None

attempt shortcuts

Determina cómo el cliente de NHRP decide cuándo originar solicitudes de resolución.

Valores válidos: Y, N, Data-rate (Velocidad de datos).

Y Sí. Intenta siempre establecer un VC de atajo creando una Next Hop Resolution Request y enviándola a la estación del salto siguiente.

N No. Nunca intenta establecer un atajo. Esta opción inhabilita básicamente la función de cliente en el direccionador. Este valor puede usarse en un direccionador intermedio (un direccionador que no sea un punto de entrada a la red NBMA para el tráfico direccionado) para eliminar el “efecto dominó”, donde el tráfico que

Mandatos de configuración avanzada de NHRP (Talk 6)

sigue la vía de acceso direccionada presenta NHRP Resolution Requests en cada direccionador de NHRP situado a lo largo de la vía de acceso.

Data-rate

Intenta establecer un atajo únicamente después de que se haya alcanzado el umbral de velocidad de datos.

Nota: Este valor puede evitar la creación de VCC para tráfico de “una ocasión” como, por ejemplo, indicadores de detección de condición de excepción de SNMP que se envían a un gestor de SNMP.

Valor por omisión: Data-rate.

Ejemplo: `set attempt`

Try shortcut VCs? (Yes, No, Data-rate) [Data-rate]?

holding time

Establece el tiempo de retención en minutos.

El parámetro del tiempo de retención se usa para estas funciones:

- Cuando el direccionador responde a una Next Hop Resolution Request con información acerca de sí mismo (es decir, el direccionador se va a convertir en el atajo del salto siguiente), el tiempo de retención se envía al peticionario como el período de tiempo en que se considerará válida la información.
- Cuando el direccionador responde a una Next Hop Resolution Request con información acerca de otra estación NBMA de la que no se supo usando NHRP (por ejemplo, la estación de destino es un dispositivo ATM con una dirección IP en una de las subredes de dispositivo), el tiempo de retención se envía al peticionario como el período de tiempo en que se considerará válida la información.

Valores válidos: De 1 a 60 minutos.

Valor por omisión: 20 minutos.

Ejemplo: `set hold`

Holding time (in minutes) [20]?

data-rate threshold

Establece el umbral de velocidad de datos en paquetes/segundo.

Este umbral se usa cuando el parámetro **attempt shortcuts** se establece en **Data-rate**.

Cuando el tráfico esté destinado a una estación en concreto, pero la velocidad es inferior a este umbral, el direccionador no intentará establecer métodos abreviados. (Dicho de otra forma, no generará Next Hop Resolution Requests y los enviará al salto siguiente de la vía de acceso direccionada). Cuando la velocidad del tráfico supere el umbral, el direccionador intentará establecer un atajo. Si puede crear satisfactoriamente un atajo, éste se usará incluso si el tráfico cae por debajo del umbral. El recorrido seguirá utilizándose hasta que el tráfico se detenga por un período de tiempo. Esto se hace para evitar ir adelante y atrás, de la vía de acceso direccionada al atajo y viceversa si el tráfico es esporádico.

Mandatos de configuración avanzada de NHRP (Talk 6)

Valores válidos: Mínimo 1 paquete/segundo. Máximo 5120 paquetes/segundo.

Valor por omisión: 10 paquetes/segundo.

Ejemplo: `set data`

Data-rate threshold in packets/second [10]?

extensions

Establece el uso de la extensión NHRP seleccionada en *yes* (sí) o *no*.

Forward transmit NHS (valor por omisión: no)

Reverse transmit NHS (valor por omisión: no)

Responder Address (valor por omisión: no)

Lane Shortcuts (valor por omisión: yes)

Valores válidos: yes o no

Ejemplo: `set ext lane`

Use LANE shortcuts extension [Yes]?

cache size *resolución* **O** *registro* **O** *depuración servidor*

Establece el número máximo de entradas de la antememoria seleccionada.

Los tamaños de la antememoria pueden seleccionarse entre los siguientes:

resolution cache

Este parámetro le permite determinar el número de entradas en la antememoria para las funciones cliente. Cada entrada de la antememoria contiene la correlación de la dirección de protocolo con la dirección NBMA que puede usarse para crear VC de atajo. Las entradas están en la antememoria cuando el direccionador:

- Ha resuelto satisfactoriamente una dirección de protocolo a una dirección NBMA enviando Next Hop Resolution Requests.
- Ha intentado resolver una solicitud de protocolo a una dirección NBMA pero no ha recibido respuesta o ha recibido una respuesta negativa y el tiempo del temporizador asociado no se ha excedido. Estas entradas se mantienen en la antememoria para evitar que el dispositivo genere Next Hop Resolution Requests adicionales durante un período de tiempo.
- Ha recibido una solicitud de registro de un cliente y el tiempo de retención indicado en la solicitud no ha expirado.

Cuando se supera el tamaño de la antememoria, ya no se efectuarán intentos nuevos de resolver direcciones de protocolo con direcciones NBMA (dicho de otra manera, no se envían Next Hop Resolution Requests nuevas) hasta que se depuren las entradas existentes, ya sea porque el tiempo de retención se ha agotado o porque se ha recibido una solicitud de depuración específica del originador de la información. Además, cuando se supera el tamaño de la antememoria, se rechazan las Registration Requests de los clientes nuevos.

Valores válidos: De 256 a 65535 entradas.

Valor por omisión: 10000 entradas.

Ejemplo: set cache res

Number of cache entries
[10000]?

registration cache

Establece un límite en el número de entradas de registro de la antememoria de resolución. Cuando el servidor recibe una solicitud de registro, comprueba si el número de registros de clientes de NHRP está por debajo de este límite antes de añadir una entrada de registro en la antememoria de resolución.

Valores válidos: De 256 a 16384 entradas.

Valor por omisión: 10000 entradas.

Ejemplo: set cache reg

Number of cache entries
[10000]?

server purge cache

Este parámetro le permite determinar el número de entradas en la antememoria de depuración del servidor. Una entrada de esta antememoria representa una dirección de protocolo de destino y un cliente al que el servidor ha proporcionado información Authoritative NBMA (NBMA de autorización) para dicho destino.

La dirección de destino puede representar al mismo servidor, a dispositivos de subredes con los que el servidor esté conectado, clientes de NHRP que se han registrado en el servidor o direccionadores a los que se ha anunciado un atajo R2R. El direccionador usa la información de estas entradas de antememoria para notificar a los clientes que depuren la información de dirección que se ha vuelto no válida antes de que se agote el temporizador de retención.

Cuando el tamaño de la antememoria de depuración del servidor se supere, el servidor rechazará las Authoritative Next Hop Resolution Requests.

Valores válidos: De 256 a 65535 entradas.

Valor por omisión: 10000 entradas.

Ejemplo: set cache serv

Number of cache entries
[10000]?

shortcuts to ATMARP clients

Permite o no permite métodos abreviados a clientes de ATMARP.

Puede usarse este parámetro para permitir o no permitir que el servidor ponga los métodos abreviados en manos de clientes de ATMARP nativos que no dan soporte a NHRP. Este parámetro puede ser necesario si estos clientes no son capaces de dar soporte a un gran número de VC. Use la opción "Exclude List" si es necesario no dar permiso a los métodos abreviados de forma selectiva a algunos clientes o subredes.

Ejemplo: set shortcut

Allow shortcuts to Classical IP clients? [Yes]:

Acceso al proceso de supervisión de NHRP

Para acceder al indicador de supervisión de NHRP:

1. En el indicador de supervisión del operador (*), escriba **talk 5** y pulse Intro.
2. En el indicador +>, escriba **protocol nhrp** y pulse Intro.
3. Aparecerá el indicador NHRP>.

Mandatos de supervisión de NHRP

Esta sección explica todos los mandatos de supervisión de NHRP tal como se muestran en la Tabla 111. Entre los mandatos en el indicador NHRP>.

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte la sección "Cómo obtener ayuda" en la página xxix.
Box Status	Muestra el estado de habilitación/inhabilitación de NHRP.
Interface Status	Muestra el estado de la interfaz de NHRP.
Statistics	Muestra las estadísticas de la interfaz de NHRP.
Cache	Muestra las entradas de antememoria de la resolución de NHRP.
Server_purge_cache	Muestra las entradas de server_purge_cache.
MIB	Muestra información de MIB.
LANE Shortcuts	Muestra las entradas de atajo LANE.
CONFIG Parameters	Muestra, cambia o restablece información de configuración de NHRP.
Reset	Vuelve a configurar dinámicamente protocolo o interfaces de HRPP.
Exit	Le devuelve al nivel de mandatos anterior. Consulte la sección "Cómo salir de un entorno de nivel inferior" en la página xxix.

Box Status

Use el mandato **box status** para visualizar el estado de NHRP tal como se ha configurado para su entrega (por ejemplo, no se ha definido explícitamente ninguna interfaz).

Sintaxis:

box-status

Ejemplo:

```
box status
Box level NHRP is ON by config
```

Interface Status

Use el mandato **interface status** para visualizar el estado de NHRP en las interfaces.

Sintaxis:

interface-status

Ejemplo:

```
interface status
  Interface 0: UP (NHRP enabled)
  Interface 1: UP (NHRP disabled)
  Interface 2: DOWN
  Interface 3: UP (NHRP LANE Shortcut Interface)
```

Statistics

Use el mandato **statistics** para visualizar estadísticas NHRP para todas las interfaces o para una interfaz específica.

Sintaxis:

```
statistics          all
                    interface
```

all Establece una lista de estadísticas NHRP en todas las interfaces.

Ejemplo: statistics all

Se produce lo mismo que en el caso del mandato **statistics interface** tal como aparece en el ejemplo siguiente.

interface Establece una lista de las estadísticas de NHRP de una interfaz especificada.

Ejemplo: statistics interface

```
Interface number [0]? 0

Statistics for Interface 0
-----
Field Description                               Value
-----
Inbound Requests                               5
Outbound Requests                              3
Inbound Replies                                3
Outbound Replies                               5
Inbound Registers                              0
Outbound Registers                             0
Inbound Error Packets                          0
Inbound Error Indication Packets               0
Outbound Error Indication Packets              0
Reply Forwards                                 0
Unrecognized Options                           0
Registration Overflows                         0
ProtocolErrors                                 0
Negative Outbound Replies                      0
Inbound Packets on NHRP disabled interface     0
'Send_to_me' Outbound Replies                  0
Inbound Purges                                 0
Outbound Purges                                2
```

Cache

Use el mandato **cache** para visualizar todas las entradas de antememoria de resolución NHRP o una entrada de antememoria específica identificada por una dirección de destino.

Sintaxis:

```
cache          list  
                entry
```

list Lista las entradas de antememoria de NHRP.

entry Lista una entrada de antememoria de NHRP específica.

Ejemplos:

```
cache list  
Total Client Cache Entries = 3  
  
NHRP Client Cache Entries  
=====
```

Dest Address	NextHop Address	State	Htime	MTU	Net
5.5.5.1	5.5.5.1	Act	1121	4490	1
5.5.5.2	5.5.5.2	Inact	1185	4490	1
6.6.6.1	6.6.6.1	Act	602	9180	0

```
cache entry  
Enter destination address [0.0.0.0]? 6.6.6.1  
Destination: 6.6.6.1  
NextHop: 6.6.6.1  
ATM Address: 39840F00000000000000000000410005A00DEADCA  
State: Act  
Net: 0  
HoldingTime: 433 seconds  
MTU size: 9180  
Flags: 0x00420000
```

Server_purge_cache

Use el mandato **server_purge_cache** para listar todas las entradas de antememoria de depuración del servidor NHRP.

Sintaxis:

```
server_purge_cache
```

MIB

Use el mandato **MIB** para visualizar información relacionado con la MIB de NHRP.

Sintaxis:

```
mib          list ...  
                entry ...
```

list Lista las entradas mib de NHRP para:

- Tabla de servidores
- Tabla de clientes
- Tabla de estadísticas del servidor del salto siguiente (NHS)

Mandatos de supervisión de NHRP (Talk 5)

```
LANE Shortcut Interface number [0]? 1
Enter IP address of next hop [0.0.0.0]? 5.5.5.1
Next Hop Addr: 5.5.5.1
Dest Mac Addr: 04-AA-AA-AA-AA-01
ATM Address: 39840F0000000000000000000310005A00DEAD02
Media type: Token Ring
VPI/VCI: 0/34
Holding Time: 20 minutes
MTU size: 4490
RI Field:064001020203
```

disallowed

Muestra todas las entradas de atajo LANE no permitidas.

Cualquier dirección ATM que aparezca listada indicará que la NHRP LANE Shortcut Interface recibió datos de la dirección ATM. Esto no está permitido ya que todos los VCC de NHRP LANE Shortcut Interface se usarán únicamente para transmitir datos a un LEC del otro extremo. Si el LEC intenta enviar datos sobre un VCC mediante una NHRP LANE Shortcut Interface, se desactivará el VCC y no se volverán a establecer más métodos abreviados LANE a dicho LEC.

Una vez corregida la condición que produjo que la NHRP LANE Shortcut Interface recibiera datos, el dispositivo deberá reiniciarse para que los métodos abreviados NHRP LANE vuelvan a utilizar la dirección ATM.

Ejemplo: lan dis

```
LAN Shortcut Interface #: 2, ATM Network Interface #: 0
=====
Atm Address
-----
39840F0000000000000000000310005A00DEAD02
```

CONFIG Parameters

Use el mandato **config parameters** para acceder a los menús de mandatos de los parámetros de configuración de NHRP **display**, **change** o **reset**.

Tabla 112. Resumen de los parámetros de configuración de NHRP

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte la sección "Cómo obtener ayuda" en la página xxix.
Display	Muestra los parámetros de configuración de conmutación de rutas y NHRP.
Change	Permite cambiar dinámicamente los parámetros de configuración de NHRP sin influir en la configuración estática.
Reset	Lee el parámetro de configuración de la configuración estática y lo usa durante el tiempo de ejecución del direccionador.

Display

Use el mandato **display** para visualizar los parámetros de configuración de conmutación de rutas y NHRP.

Sintaxis:

```
display          nhrp
```


nhrp Muestra los parámetros de configuración de NHRP, incluyendo los parámetros generales, los tamaños de antememorias, el uso de extensiones, la lista de exclusión y los métodos abreviados no permitidos de direccionador a direccionador.

Change

Use el mandato **change** para cambiar los parámetros de configuración de NHRP actuales. Consulte “Set” en la página 456 para obtener una descripción de los parámetros de configuración.

Sintaxis:

```
change          protocol_access_control_usage
                  attempt_shortcuts
                  holding_time
                  data-rate_threshold
                  cache_size
                  extensions
                  shortcuts_to_atmarp_clients
```

Reset

Use el mandato **reset** para restablecer el valor del parámetro de configuración dinámica en el valor de la configuración estática. Consulte “Set” en la página 456 para obtener una descripción de los parámetros de configuración.

Sintaxis:

```
reset          protocol_access_control_usage
                  attempt_shortcuts
                  holding_time
                  data-rate_threshold
                  cache_size
                  extensions
                  shortcuts_to_atmarp_clients
                  exclude_list
                  disallowed_router-to-router
```

Reset

Use el mandato **reset** para volver a configurar dinámicamente el protocolo NHRP o una interfaz. Un mandato reset hace que los valores de configuración estáticos aplicables se usen.

Sintaxis:

```
reset          interface
                  nhrp
```

Rastreo de paquetes de NHRP

- nhrp** Restablece estadísticas, interfaces y parámetros de configuración de NHRP en los valores de configuración estáticos. Esto equivale a un inicio en frío de NHRP.
- interface** Desactiva la interfaz de NHRP y activa la interfaz con nuevos valores de configuración estática de la interfaz.

Rastreo de paquetes de NHRP

El rastreo de paquetes de NHRP puede activarse desde el sistema de anotación cronológica de sucesos (ELS), que es una parte integral del sistema operativo del direccionador. Consulte “Using and Configuring the Event Logging System” y “Monitoring the Event Logging System” en el manual *Guía del usuario de software*.

El mecanismo de rastreo de paquetes NHRP da soporte a la opción “set trace decode on”. Esta opción permite que la producción de rastreo de paquetes NHRP pueda interpretarse para verla. También pueden rastrearse las tramas de control sobre LSI aparte de los paquetes del protocolo NHRP. Para obtener detalles sobre el uso de la función de rastreo, consulte la descripción del mandato **trace** en “Monitoring the Event Logging System” en el manual *Guía del usuario de software*.

Los paquetes del protocolo NHRP se identifican mediante el suceso 19 y los paquetes de control de LSI mediante el suceso 113.

Ejemplo de producción de rastreo núm. 1:

```
Dir:OUTGOING Time:0.0.48.88 Trap:6035
Comp:NHRP Type:UNKNOWN Port:1 Circuit:0x000000 Size:160
-----
** NHRP/MPOA Frame **
AddressFamily:ATM_NSAP ProtocolType:IPv4 HopCount:64 PacketSize:160
Checksum:0x03F4 ExtensionOffset:0x0038 Version:1 PktType:ResolutionRequest
SrcAddrTL:20 SrcSubAddrTL:0 SrcProtoLen:4 DstProtoLen:4
Flags:requester is a router Flags:want authoritative only Flags:want unique
only ReqID:1
Src NBMA:39840F0000000000000000000610005A019600C9
Src Protocol Addr: 6.6.6.1 Dest Protocol Addr: 3.3.3.2
0038: 00 08 00 1C 08 00 5A 00 00 01 00 0A 00 00 00 00 | .....Z..... |
0048: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ..... |
0058: 00 08 00 34 08 00 5A 00 00 01 00 0C 00 00 00 00 | ...4..Z..... |
0068: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ..... |
0078: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ..... |
0088: 00 00 00 00 00 00 00 00 00 08 00 08 08 00 5A 00 | .....Z. |
0098: 00 01 00 06 80 00 00 00 | ..... |
```

Ejemplo de producción de rastreo núm. 2:

```

Dir:INCOMING Time:0.0.50.69 Trap:6035
Comp:NHRP Type:UNKNOWN Port:1 Circuit:0x000000 Size:202
-----
** NHRP/MPOA Frame **
AddressFamily:ATM_NSAP ProtocolType:IPv4 HopCount:63 PacketSize:202
Checksum:0xEC88 ExtensionOffset:0x005C Version:1 PktType:ResolutionReply
SrcAddrTL:20 SrcSubAddrTL:0 SrcProtoLen:4 DstProtoLen:4
Flags:requester is a router Flags:authoritative info Flags:requested info
unique ReqID:1
Src NBMA:39840F0000000000000000000000000610005A019600C9
Src Protocol Addr: 6.6.6.1 Dest Protocol Addr: 3.3.3.2
1483 VCC Shortcut Information (CIE) follows:
  CIE Code:0 Prefix:32 MTU:4376 Htime:180 Preference:254
  CIE NBMA:39840F0000000000000000000000000310005A01950103
  CIE Protocol Addr: 3.3.3.1
005C: 00 08 00 1C 08 00 5A 00 00 01 00 0B 00 00 00 01 | .....Z..... |
006C: 97 00 01 04 03 03 03 02 11 18 90 00 5A 01 94 00 | .....Z... |
007C: 00 08 00 34 08 00 5A 00 00 01 00 0D 00 B4 14 00 | ...4..Z..... |
008C: 39 84 0F 00 00 00 00 00 00 00 00 00 03 10 00 5A | 9.....Z |
009C: 01 95 01 03 00 00 00 00 00 00 00 00 00 00 00 00 | .....Z. |
00AC: 00 00 00 00 00 00 00 00 00 08 00 0E 08 00 5A 00 | .....Z. |
00BC: 00 01 00 07 06 A0 00 80 00 20 80 00 00 00 00 00 | ..... |

```

NHRP Soporte de reconfiguración dinámica del servidor NHRP

Esta sección describe la reconfiguración dinámica (DR) en la medida en que afecta a los mandatos de Talk 6 y Talk 5.

Delete Interface de CONFIG (Talk 6)(Suprimir interfaz)

El servidor NHRP da soporte al mandato **delete interface** de CONFIG (Talk 6), teniendo en cuenta lo siguiente:

- No se puede suprimir el LANE Shortcut Interface de NHRP con el mandato **delete interface**. Use la opción de config **disable nhrp** para suprimir LANE Shortcut Interface de NHRP.

Activate Interface de GWCON (Talk 5)(Activar interfaz)

El servidor NHRP da soporte al mandato **activate interface** de GWCON (Talk 5), teniendo en cuenta lo siguiente:

- El LSI (LANE Shortcut Interface) de NHRP asociado con cada interfaz física de ATM se activa automáticamente después de la activación de la interfaz física de ATM asociada.

Todos los mandatos del servidor NHRP específicos de la interfaz están soportados por el mandato de GWCON (Talk 5) **activate interface**.

Reset Interface de GWCON (Talk 5)(Restablecer interfaz)

El servidor NHRP da soporte al mandato de GWCON (Talk 5) **reset interface**, teniendo en cuenta lo siguiente:

- No puede restablecer el tipo de interfaz LANE Shortcut Interface de NHRP sin reiniciar.

Todos los mandatos del servidor NHRP específicos de la interfaz están soportados por el mandato de GWCON (Talk 5) **reset interface**.

Uso de IP Versión 6 (IPv6)

Este capítulo describe cómo usar IPv6.

Visión general de IPv6

IP Versión 6 (IPv6) es una versión nueva de Internet Protocol. Se ha diseñado para que suceda a IP Versión 4 (IPv4). La lista siguiente indica algunas de las ventajas que IPv6 proporciona:

- Un espacio de dirección grande
IPv6 usa una dirección de 128 bits.
- Direccionamiento
Mediante el tamaño de dirección grande, IPv6 proporciona un esquema de dirección jerárquica que le permite crear una jerarquía de direccionamiento flexible.
- Configuración fácil
NDP proporciona configuración automática del sistema principal.
- Seguridad
IPv6 convierte en obligatoria la seguridad de IP.
- Soporte para tráfico multimedia
La cabecera de IPv6 tiene campos de etiqueta de flujo y de prioridad para acomodar una calidad de servicio integrada.
- Simplificación
La cabecera de IPv6 es fija y simplificada. Ya no es necesario el direccionador para efectuar una fragmentación que simplifique el proceso de paquetes. Además, los datos de tipos de opciones se implementan en cabeceras de extensión que sólo reciben proceso del nodo de destino.

Comparación de IPv6 con IPv4

IPv6 incluye varios cambios comparado con IPv4. Los cambios más significativos son:

- Dirección
- Formato de cabecera
- MTU mínima
- Mandatory Path MTU discovery
- Seguridad de IP obligatoria
- Neighbor Discovery Protocol (NDP)

Direccionamiento de IPv6

El direccionamiento de IPv6 aumenta la dirección, que pasa de 32 bits a 128 bits. Este aumento permite que haya más grados de jerarquía que capas básicas de la red, subred y sistema principal.

Las direcciones de IPv6 pertenecen a una de las tres categorías siguientes:

- Difusión individual. Se entrega un paquete a la interfaz identificada por la dirección.
- Difusión múltiple. Se envía un paquete a todos los miembros del grupo de difusión múltiple identificado por la dirección.
- Única difusión. Se envía un paquete únicamente al miembro más cercano del grupo identificado por la dirección.

En IPv6, se ha sustituido el direccionamiento de difusión por el direccionamiento de difusión múltiple.

Formato de dirección de IPv6

La dirección de IPv6 está compuesta por 128 bits. Estos bits se escriben como ocho números enteros de 16 bits separados por el signo de dos puntos.

Ejemplo:

ABCD:1234:0000:1234:5555:FFEE:7777:0123

Se pueden utilizar las reglas de simplificación siguientes:

- Saltar los ceros iniciales.

Ejemplo:

ABCD:1234:0:1234:0:FFEE:7777:123

- Dentro de una dirección, un conjunto de números consecutivos y nulos de 16 bits puede sustituirse por dos signos de dos puntos.

Ejemplo:

ABCD:1234::1234:5555:FFEE:7777:123

1234::7899

Los signos de dos puntos dobles sólo se pueden usar una vez dentro de la dirección.

- Cuando trate con un entorno mixto de nodos IPv4 e IPv6, puede usar la forma **x:x:x:x:d.d.d.d**

donde las x son valores hexadecimales de las seis partes de 16 bits más significativas de la dirección y las d son valores decimales de las cuatro partes de 8 bits menos significativas de la dirección en la representación de IPv4 estándar.

Ejemplo:

ABCD:1234::1234:5555:FFEE:1.2.3.4

::1.2.3.4

Representación textual de prefijos de direcciones

Un prefijo de dirección de IPv6 se representa mediante la notación:

Dirección-IPv6/longitud-prefijo

La dirección de IPv6 puede usar cualquiera de las notaciones listadas en “Formato de dirección de IPv6” en la página 470 y la longitud de prefijo es un valor decimal que especifica cuántos de los bits contiguos situados más a la izquierda de la dirección forman el prefijo.

Ejemplo:

ABCD:1234::1234:5555:FFEE:1.2.3.4/64

Formato de cabecera de IPv6

La cabecera de IPv6 tiene un total de 8 campos, en la que se eliminan algunos campos IPv4 como el de suma de comprobación y el de fragmentación.

MTU mínima de IPv6

La MTU mínima para IPv6 tiene 1280 bytes. No se puede habilitar IPv6 en una interfaz con una MTU con menos de 1280 bytes.

Path MTU Discovery obligatorio en IPv6

Path MTU Discovery es un protocolo que permite a un sistema principal determinar el paquete de tamaño máximo que atravesará satisfactoriamente una vía de acceso a un destino sin fragmentarse. A medida que se generen y envíen paquetes desde el sistema principal, la MTU de la interfaz de salida en particular a la que se envía el paquete, estará disponible.

Si el paquete se adapta a la interfaz de salida, ya sea en su totalidad o en fragmentos, se transmitirá. Si un direccionador de la vía de acceso necesita reenviar este paquete a una red con una MTU más pequeña que el tamaño del paquete, éste se eliminará y se enviará un mensaje ICMP al originador del paquete en el que se indica el tamaño necesario del paquete para que quepa en la red de salida del direccionador intermedio. El sistema principal que reciba este mensaje ajustará el tamaño de los paquetes posteriores reenviados en la vía de acceso. Este proceso puede producirse varias veces antes de que el paquete alcance el destino final. Una vez el paquete haya alcanzado su destino, los paquetes posteriores no deberán eliminarse porque el tamaño del paquete sea demasiado grande.

Dado que la ruta puede cambiar dinámicamente, la MTU de la vía de acceso puede aumentar y necesitar, por lo tanto, un ajuste en el nodo del sistema principal. Se asigna una edad a las MTU de la vía de acceso de las que se tiene conocimiento y el proceso de Path MTU Discovery vuelve a producirse. Esto permite que el tamaño del paquete transmitido reaccione a la naturaleza dinámica de las rutas de la red.

Path MTU Discovery es obligatorio ya que la fragmentación no está permitida en los direccionadores de tránsito.

Si el dispositivo actúa como direccionador de tránsito, no reenviará paquetes de tamaño superior a la MTU de la red de salida. Generará un mensaje ICMP Packet Too Big (Paquete ICMP demasiado grande) y lo enviará al origen del paquete.

El mandato **enable path-mtu-discovery** en el indicador IPv6 Config> puede usarse para habilitar o inhabilitar path MTU discovery. Por omisión, path MTU discovery se habilita.

Use el mandato **set path-mtu-aging-timer** en el indicador IPv6 Config> para especificar el tiempo de envejecimiento de las MTU de la vía de acceso que se han determinado.

Seguridad obligatoria de IPv6

Un nodo IPv6 debe dar soporte a la seguridad IP. Esta seguridad puede habilitarse o inhabilitarse. Consulte “Using IP Security” (Uso de la seguridad IP) y “Configuring and Monitoring IP Security” (Configuración y supervisión de la seguridad IP) en el manual *Using and Configuring Features* para obtener información adicional sobre la seguridad IP.

1. Use el mandato **add packet** en el indicador IPv6 Config> para añadir un filtro de paquetes.
2. Use el mandato **update packet** en el indicador IPv6 Config> para actualizar el filtro de paquetes.
3. Use el mandato **add access** en el indicador Packet-filter 'nombre_filtro' Config> para añadir controles de acceso.
4. Use el mandato **set acc on** en el indicador IPv6 Config> para habilitar el control de accesos.

IPv6 Neighbor Discovery Protocol (NDP)

IPv6 usa NDP para realizar la configuración automática. NDP permite que los nodos de IPv6 que estén en el mismo enlace descubran la presencia respectiva, a fin de determinar las direcciones de la capa de enlace de cada uno, encontrar direccionadores y mantener información de accesibilidad sobre las vías de acceso a los vecinos activos.

Router y Prefix Discovery

Los sistemas principales usan Router Discovery (descubrimiento de direccionadores) para descubrir direccionadores que residen en un enlace conectado. Cada direccionador ejecuta, periódicamente, una difusión múltiple de un paquete Router Advertisement (anuncio de direccionador), si está configurado, en el que anuncia su disponibilidad. Los anuncios de direccionador contienen una lista de prefijos usados para la determinación de enlaces activos y la configuración de direcciones autónomas. Los sistemas principales pueden usar los prefijos de enlace activo anunciados para determinar cuándo, el destino de un paquete, está en el enlace o más allá de un direccionador.

Configuración automática de direcciones

Los anuncios de direccionadores permiten a estos informar a los sistemas principales sobre cómo ejecutar la configuración automática de direcciones. Los direccionadores pueden especificar si los sistemas principales usan la configuración de direcciones autónomas (sin estado) o estatal.

Resolución de direcciones

Los direccionadores efectúan la resolución de direcciones ejecutando una difusión múltiple de un mensaje de solicitud de vecino que pide al nodo de destino que devuelva su dirección de capa de enlace. La dirección de la capa de enlace se devuelve en un anuncio de vecino de una difusión individual. Al incluir la dirección de la capa de enlace en el mensaje de solicitud de vecino, un par único de mensajes de solicitud y respuesta, el iniciador del mensaje y el destinatario pueden determinar las direcciones de la capa de enlace de ambos.

Detección de inaccesibilidad de vecinos

NDP puede detectar el fallo de un vecino o el de la vía de reenvío al vecino. Cuando no se ha recibido una confirmación positiva de un vecino para un intervalo de tiempo, el nodo ejecuta una prueba activamente en el vecino con mensajes de solicitud de vecino de una difusión individual para verificar que la vía de acceso de reenvío sigue funcionando.

Redirección

Si la dirección de origen del paquete y del salto siguiente están en la misma red, un direccionador puede enviar un mensaje de redirección informando al remitente que el salto siguiente es un vecino.

Use el mandato **p ndp** en el indicador `Config>` para configurar parámetros de NDP.

Función de túnel de IPv6 sobre IPv4

La función de túnel de IPv6 sobre IPv4 le permite migrar de redes IPv4 a redes IPv6 sin tener que actualizar, simultáneamente, todo el equipo para dar soporte a IPv6. Esta función permite que las tramas de IPv6 crucen una red IPv4 y lleguen a un destino IPv6. La trama de IPv6 se encapsula en una trama de IPv4 y se reenvía a través de la red IPv4 a un destino IPv4 específico llamado punto final del túnel. En este punto final, se extrae el paquete de la cápsula y se reenvía al destino IPv6 final.

Añadir un túnel configurado hace que se añada una interfaz virtual. Esta interfaz se trata por IPv6 como si fuera una interfaz normal y el RIP puede usarla para el establecimiento de rutas.

Use el mandato **add tunnel** en el indicador `IPv6 Config>` para añadir un IPv6 sobre túnel IPv4.

Protocol Independent Multicast (PIM)

Consulte la sección “Uso de PIM” en la página 517 si desea información acerca del uso del protocolo PIM.

Configuración y supervisión de IPv6

Este capítulo describe cómo usar los mandatos de funcionamiento y configuración de IPv6 e incluye las secciones siguientes:

- “Acceso al entorno de configuración de IPv6”
- “Mandatos de configuración de IPv6”
- “Acceso al entorno de supervisión de IPv6” en la página 496
- “Mandatos de supervisión de IPv6” en la página 496
- “Soporte de reconfiguración dinámica de IPv6” en la página 504

Acceso al entorno de configuración de IPv6

Siga el procedimiento siguiente para acceder al proceso de configuración de IPv6.

1. En el indicador OPCON, entre **talk 6**. (Para obtener información detallada sobre este mandato, consulte *The OPCON Process and Commands* (Proceso y mandatos de OPCON) en la Guía del usuario de software.) Por ejemplo:

```
* talk 6
Config>
```

Después de entrar el mandato **talk 6**, el indicador CONFIG (Config>) aparecerá en el terminal. Si el indicador no aparece cuando entre por primera vez la configuración, pulse de nuevo **Retorno**.

2. En el indicador CONFIG, entre el mandato **p ipv6** para obtener el indicador IPv6 Config>.

Mandatos de configuración de IPv6

Para configurar IPv6, entre los mandatos en el indicador IPv6 Config>.

Tabla 113 (Página 1 de 2). Resumen de los mandatos de configuración de IPv6

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte la sección “Cómo obtener ayuda” en la página xxix.
add	Añade una dirección, rutas filtradas, filtros de paquetes, ruta o túnel.
change	Cambia una dirección, rutas filtradas, filtros de paquetes, ruta o túnel.
delete	Suprime una dirección, rutas filtradas, filtros de paquetes, ruta o túnel.
disable	Inhabilita las redirecciones icmp, el filtro de paquetes o el descubrimiento de la MTU de la vía de acceso.
enable	Habilita las redirecciones ICMP, los filtros de paquetes o el descubrimiento de MTU de la vía de acceso.
list	Lista la configuración.
move	Mueve el control de acceso.

Mandatos de configuración de IPv6 (Talk 6)

Mandato	Función
set	Establece los valores de configuración asociados a túneles automáticos, tamaños de almacenamiento intermedio de antememorias de vías de acceso de reenvío rápido, pasarelas por omisión, MLD, temporizadores de antigüedad de la MTU, el tamaño del almacenamiento intermedio de ensamblaje de paquetes, el tamaño de las tablas de direccionamiento, el id de direccionadores y el tiempo de vida del direccionador.
update	Actualiza el filtro de paquetes.
Exit	Le devuelve al nivel de mandatos anterior. Consulte la sección "Cómo salir de un entorno de nivel inferior" en la página xxix.

Add

Use el mandato **add** para añadir una dirección de IPv6, rutas filtradas, filtros de paquetes, rutas o túneles de IPv6 sobre IPv4.

add *access-control*
 address prefijo dirección red
 leaked-routes destino
 packet-filter nombre interfaz
 route coste de pasarela de la máscara de destino...
 tunnel prefijo destino direcciónr direcciónlocal coste ttl fragmen-
 tación

Ejemplo:

```
IPv6 config>add address
Which net is this address for [0]? 5
New address []? 1::2
Prefix length must between 8 and 128 [128]?
```

```
IPv6 config>add leaked
IPv4 destination []? 1.2.3.4
Address mask [255.0.0.0]? 255.255.255.255
```

```
IPv6 config>add packet-filter
Packet-filter name []? pktf01
Filter incoming or outgoing traffic [IN]
Which interface is this filter for [0]? 3
```

```
IPv6 config>add route
IPv6 destination []? 8::9
Prefix length must between 8 and 128 [8]? 128
Via gateway 1 at []? 1::2
Cost [1]?
Via gateway 2 at []? 2::3
Cost [1]? 1000
Via gateway 3 at []? 3::4
Cost [1]? 10000
Via gateway 4 at []? 4::5
Cost [1]? 10
```

```
IPv6 config>add tunnel
Add a static route through this tunnel? [Yes[:
IPv6 destination network []? 3::4
Prefix length must between 0 and 128 [64]? 128
IPv4 tunnel remote address []? 1.2.3.4
IPv4 tunnel local address []? 2.3.40.0
Cost [1]?
TTL value [64]?
Allow fragmentation in tunnel?(Yes or [No]):
```

access-control

Añade control de acceso

access control type

Indica lo que se hace con los paquetes que coinciden con los parámetros de la norma de control de acceso.

E Excluyente; los paquetes que coincidan se descartarán.

I Incluyente; los paquetes que coincidan recibirán proceso adicional del direccionador.

Internet source

Dirección Internet de origen.

Valores válidos: Cualquier dirección de internet válida

Valores por omisión: Ninguno

Source Prefix length

Especifica la longitud del prefijo de la dirección de origen de Internet.

Valores válidos: De 0 a 128

Valores por omisión: 128

Internet destination

Dirección Internet de destino.

Valores válidos: Cualquier dirección de internet válida

Valor por omisión: Ninguno

Destination Prefix length

Especifica la longitud del prefijo de la dirección de destino de Internet.

Valores válidos: De 0 a 128

Valores por omisión: 128

Starting protocol number

Especifica el número de protocolo de inicio de un rango de números de protocolo. Entre un 0 para seleccionar todos los protocolos.

Algunos números de protocolo comunes son:

- 1 para ICMP
- 6 para TCP
- 17 para UDP
- 89 para OSPF
- 50 para ESP-Encryption
- 51 para AH-Encryption

Valores válidos: de 0 a 255

Valores por omisión: 0

Ending protocol number

Especifica el número de protocolo final de un rango de números de protocolo. Entre un 0 para seleccionar todos los protocolos.

Algunos números de protocolo comunes son:

- 1 para ICMP
- 6 para TCP
- 17 para UDP
- 89 para OSPF
- 50 para ESP-Encryption
- 51 para AH-Encryption

Valores válidos: de 0 a 255

Valores por omisión: el valor especificado en el parámetro **starting protocol number**

Starting destination port number

Especifica el número del puerto de inicio de un rango de números de puerto de destino TCP/UDP. Estos parámetros sólo son válidos si el rango de números de protocolo incluye 6 (para TCP) o 17 (para UDP). No se tendrán en cuenta estos parámetros para los paquetes en los cuales el número de protocolo no sea 6 ó 17.

Algunos números de puerto usados normalmente son:

- 21 para FTP
- 23 para Telnet

25 para SMTP
513 para rlogin
520 para RIP para IPv4
521 para RIP6 para IPv6

Valores válidos: De 0 a 65535

Valor por omisión: 0

Ending destination port number

Especifica el número del puerto final de un rango de números de puerto de destino TCP/UDP. Estos parámetros sólo son válidos si el rango de números de protocolo incluye 6 (para TCP) o 17 (para UDP). No se tendrán en cuenta estos parámetros para los paquetes en los cuales el número de protocolo no sea 6 ó 17.

Algunos números de puerto usados normalmente son:

21 para FTP
23 para Telnet
25 para SMTP
513 para rlogin
520 para RIP para IPv4
521 para RIP6 para IPv6

Valores válidos: De 0 a 65535

Valores por omisión: el valor especificado como **starting destination port number**

Starting source port number

Especifica el número del puerto de inicio de un rango de números de puerto de origen TCP/UDP. Estos parámetros sólo son válidos si el rango de números de protocolo incluye 6 (para TCP) o 17 (para UDP). No se tendrán en cuenta estos parámetros para los paquetes en los cuales el número de protocolo no sea 6 ó 17. Consulte la descripción de **starting destination port number** para obtener una lista de los números de puerto TCP/UDP más usados.

Valores válidos: De 0 a 65535

Valor por omisión: 0

Ending source port number

Especifica el número del puerto final de un rango de números de puerto de origen TCP/UDP. Estos parámetros sólo son válidos si el rango de números de protocolo incluye 6 (para TCP) o 17 (para UDP). No se tendrán en cuenta estos parámetros para los paquetes en los cuales el número de protocolo no sea 6 ó 17. Consulte la descripción de **starting destination port number** para obtener una lista de los números de puerto TCP/UDP más usados.

Valores válidos: De 0 a 65535

Valor por omisión: el valor especificado como **starting source port number**

address Añade una dirección de IPv6.

Mandatos de configuración de IPv6 (Talk 6)

Which net is this address for

Especifica la red a la que se añadirá la dirección IPv6.

Valores válidos: Un valor numérico que identifique una interfaz de red

Valor por omisión: 0

New address

Especifica la dirección de IPv6 nueva que se añadirá.

Valores válidos: Cualquier dirección de IPv6 válida

Valor por omisión: Ninguno

Prefix length

Valor decimal que especifica cuántos de los bits contiguos situados en el extremo izquierdo de la dirección forman el prefijo.

Valores válidos: De 8 a 128

Valor por omisión: 128

leaked-routes

Añade una ruta filtrada.

IPV4 destination

Especifica la dirección de IPv6 del destino de la ruta filtrada.

Valores válidos: Cualquier dirección de IPv6 válida

Valor por omisión: Ninguno

packet-filter

Añade un filtro de paquetes

packet-filter name

Especifica un nombre alfanumérico usado para identificar el filtro de paquetes.

Valores válidos: Cualquier serie de caracteres alfanumérica que tenga un máximo de 16 caracteres

Valor por omisión: Ninguno

Filter incoming or outgoing traffic?

Especifica si desea filtrar el tráfico de entrada o de salida.

Valores válidos: OUT (salida) o IN (entrada)

Valor por omisión: IN

which interface is this filter for

Especifica el número de la interfaz de red a la que se añadirá el filtro de paquetes.

Valores válidos: Un valor numérico que identifique las interfaces para las que IPv6 sea un protocolo válido o "a", que especifica que este filtro es para el túnel automático.

Valor por omisión: 0

route Añade una ruta.

IPv6 destination

Especifica la dirección de IPv6 del destino de la ruta.

Valores válidos: Cualquier dirección de IPv6 válida

Valor por omisión: Ninguno

Prefix length

Especifica la máscara que se aplicará a la dirección de destino.

Valores válidos: De 8 a 128 (0 está permitido si el destino IPv6 es 0::0)

Valor por omisión: 8

Via gateway 1

Especifica la dirección de IPv6 de la pasarela 1.

Valores válidos: Cualquier dirección de IPv6 válida

Valor por omisión: Ninguno

Cost

Especifica el coste de esta ruta.

Valores válidos: Un valor numérico

Valor por omisión: 1

Via gateway 2

Especifica la dirección de IPv6 de la pasarela 2.

Valores válidos: Cualquier dirección de IPv6 válida

Valor por omisión: Ninguno

Cost

Especifica el coste de esta ruta.

Valores válidos: Un valor numérico

Valor por omisión: 1

Via gateway 3

Especifica la dirección de IPv6 de la pasarela 3.

Valores válidos: Cualquier dirección de IPv6 válida

Valor por omisión: Ninguno

Cost

Especifica el coste de esta ruta.

Valores válidos: Un valor numérico

Valor por omisión: 1

Via gateway 4

Especifica la dirección de IPv6 de la pasarela 4.

Valores válidos: Cualquier dirección de IPv6 válida

Valor por omisión: Ninguno

Cost

Especifica el coste de esta ruta.

Valores válidos: Un valor numérico

Valor por omisión: 1

tunnel Añade un túnel.

Add a static route through this tunnel?

Especifica si el túnel tendrá o no una ruta estática definida.

Valores válidos: Yes (Sí) o No

Valor por omisión: Yes

IPv6 destination network

Especifica la dirección de IPv6 de la red de destino a la que se accederá mediante el túnel.

Valores válidos: Cualquier dirección de IPv6 válida

Valor por omisión: Ninguno

Prefix length

Valor decimal que especifica cuántos bits contiguos situados más a la izquierda de la dirección de IPv6 forman el prefijo.

Valores válidos: De 8 a 128

Valor por omisión: 64

IPv4 tunnel remote address

Especifica la dirección de IPv4 de las tramas IPv6 que han pasado por el túnel.

Valores válidos: Cualquier dirección IP válida (32 bits)

Valor por omisión: Ninguno

IPv4 tunnel local address

Especifica la dirección de origen de IPv4 para las tramas de IPv6 que han atravesado el túnel.

Valores válidos: Cualquier dirección IP válida (32 bits)

Valor por omisión: Ninguno

Cost

Especifica el coste asociado con el túnel que se usará durante las búsquedas de ruta para encontrar la mejor ruta al destino.

Valores válidos: De 1 a 255

Valor por omisión: 1

TTL value

Especifica el valor de tiempo de vida usado en las tramas encapsuladas para este túnel

Valores válidos: Cualquier valor numérico del rango situado entre 1 y 255

Valor por omisión: 64

Allow fragmentation in the tunnel?

Especifica si estará permitida la fragmentación en el túnel. Si especifica *yes* estará permitida la fragmentación en el túnel, en el caso de que la red IPv4 que esté usando éste no proporcione la información suficiente para que el dispositivo devuelva un mensaje "Packet Too Big" (Paquete demasiado grande) al sistema principal de IPv6.

Valores válidos: yes o no

Valor por omisión: no

Change

Use el mandato **change** para añadir un registro de control de acceso, una dirección de IPv6, rutas filtradas, filtros de paquetes, rutas o túneles.

Sintaxis:

change *access-control índice*
 address prefijo dirección red
 leaked-routes destino
 packet-filter nombre interfaz
 route coste de pasarela de la máscara de destino...
 tunnel prefijo destino direcciónr direcciónlocal coste ttl fragmen-
 tación

access-control

Cambia la configuración del control de acceso.

address Cambia una dirección.

leaked-routes

Cambia la configuración de una ruta filtrada.

packet-filter

Cambia la configuración de un filtro de paquetes.

route Cambia la configuración de una ruta.

tunnel Cambia la configuración de un túnel.

Consulte "Add" en la página 476 para obtener una descripción de los parámetros asociados al mandato **change**.

Delete

Use el mandato **delete** para eliminar un registro de control de acceso, una dirección, rutas filtradas, filtros de paquetes, rutas o túneles.

Sintaxis:

delete *access-control índice*
 address dirección
 leaked-routes destino
 packet-filter nombre
 route pasarela máscara destino
 tunnel núm.túnel

Disable

Use el mandato **disable** para inhabilitar la redirección ICMP, filtros de paquetes y path MTU discovery.

Sintaxis:

disable *icmp-redirect dirección*
 packet-filter nombre-filtro-paquetes
 path-mtu-discovery

Mandatos de configuración de IPv6 (Talk 6)

icmp-redirect

Inhabilita las redirecciones de ICMP.

packet-filter

Inhabilita un filtro de paquetes.

packet-filter name

Especifica el nombre del filtro de paquetes que se inhabilitará.

Valores válidos: Cualquier filtro de paquete configurado

Valor por omisión: Ninguno

path-mtu-discovery

Inhabilita Path MTU Discovery.

Enable

Use el mandato **enable** para habilitar redirecciones de ICMP, filtros de paquetes o path MTU discovery.

Sintaxis:

enable *icmp-redirect dirección*
 packet-filter nombre-filtro-paquetes
 path-mtu-discovery

icmp-redirect

Habilita las redirecciones de ICMP.

interface address

Especifica la dirección de la interfaz.

Valores válidos: Cualquier dirección de IPv6 válida

Valor por omisión: Null (nulo) (especifica todas las direcciones)

packet-filter

Habilita un filtro de paquetes.

packet-filter name

Especifica el nombre del filtro de paquetes que se habilitará. Este nombre se configura usando el mandato **add packet-filter**.

Valores válidos: Cualquier dirección de IPv6 válida

Valor por omisión: Ninguno

path-mtu-discovery

Habilita Path MTU Discovery, un protocolo que permite a un nodo de sistema principal determinar el paquete de tamaño máximo que seguirá un recorrido a un destino sin que sea necesario fragmentarlo.

List

Use el mandato **list** para visualizar la configuración de IPv6.

Sintaxis:

list *all*
 access-control

addresses
icmp-redirect
leaked-routes
mld
packet-filter
routes
sizes
tunnels

Ejemplo:

```

IPv6 config>list all
Interface addresses
IPv6 addresses for each interface:
  intf 0                                IP disabled on this interface
  intf 1                                IP disabled on this
interface
  intf 2                                IP disabled on this
interface
  intf 3                                IP disabled on this interface
  intf 4                                IP disabled on this interface
  intf 5  1234:1234:1234:1234:5234:6234:7234:8234/128
          1223::7:1234/8
Router-ID: 1::9
Internal IP address: 1::8

Routing

route to: 1234::1223/128
  via: 1234:0:9::8                      cost: 100
  via: 1234:0:9:8:8:7:6:8                cost: 232
  via: 1:2:3:4:5:6:7:8                   cost: 1
  via: 8:7:6:5:4:3:2:1                   cost: 1
route to: ::/0
  via: 1::8                              cost: 100
route to: 2::8:9/8
  via: 1::8                              cost: 1

Path MTU Discovery: disabled
Path MTU Aging Timer: 10 minutes

Access Control is: enabled
  
```

Mandatos de configuración de IPv6 (Talk 6)

```
IPv6 config>list addresses
IPv6 addresses for each interface:
  intf 0          IP disabled on this interface
  intf 1          IP disabled on this
interface
  intf 2          IP disabled on this
interface
  intf 3          IP disabled on this interface
  intf 4          IP disabled on this interface
  intf 5 1234:1234:1234:1234:5234:6234:7234:8234/128
              1223::7:1234/8
Router-ID: 1::9
Internal IP address: 1::8
IPv6 config>list icmp-redirect
ICMP Redirect generation for IP interface:
  intf 0          IP disabled on this interface
  intf 1          IP disabled on this
interface
  intf 2          IP disabled on this
interface
  intf 3          IP disabled on this interface
  intf 4          IP disabled on this interface
  intf 5 1234:1234:1234:1234:5234:6234:7234:8234/128 ICMP Redirect enabled
              1223::7:1234/8 ICMP Redirect enabled
  intf 6          IP disabled on this interface
  intf 7          IP disabled on this interface

IPv6 config>list leaked-routes
# IPv4 Address      Mask
IPv6 config>list mld
Net      Query Interval      Response Interval      Leave Query Interval
         (secs)              (secs)                 (secs)
---      -
5        125                  10                     1

IPv6 config>list packet-filter
List of packet-filter records:

Name      Interface  State
packet01  0          On
pack01    5          On
Access Control is: enabled
IPv6 config>list routes

route to: 1234::1223/128
  via: 1234:0:9::8          cost: 100
  via: 1234:0:9:8:8:7:6:8   cost: 232
  via: 1:2:3:4:5:6:7:8     cost: 1
  via: 8:7:6:5:4:3:2:1     cost: 1
route to: ::/0
  via: 1::8                cost: 100
route to: 2::8:9/8
  via: 1::8                cost: 1
```

```
IPv6 config>list sizes
```

```
Routing table size: 768 nets (79872 bytes)
Reassembly buffer size: 12000 bytes
Routing cache size: 64 entries
Time to live: 64
Path MTU aging timer: 10
```

```
IPv6 config>list tunnel
```

```
Tun# Remote Endpoint Local Endpoint Frag Allowed TTL Cost Net# IPv6 Address/Prefix
  1   1.2.3.4         2.3.4.5         No           100   100  7   1:2:3:4:5:6:7:8/128
IPv6 config>
```

Move

Use el mandato **move** para cambiar el orden de los registros de control de acceso configurados.

Sintaxis:

```
move          access-control
```

Index of control to move

Seleccione el número de índice del registro de control de acceso que desea mover.

Move record AFTER record number

Seleccione el número de índice del registro de control de acceso que desea que este registro siga.

Are you sure that this is what you want to do

Le permite confirmar que la instrucción de movimiento es correcta.

Set

Use el mandato **set** para establecer parámetros de configuración.

Sintaxis:

```
set          access-control
             automatic-tunnel-parameters ttl/fragmentación/cuenta saltos
             cache-size núm.entradas
             default ...
             internal-ip-address
             mld ...
             path-mtu-aging-timer
             reassembly-size
             router-id
             routing núm.redes
             ttl
```

Ejemplo:

Mandatos de configuración de IPv6 (Talk 6)

```
IPv6 config>set au
TTL value [64]?
Allow fragmentation in tunnel?(Yes or [No]):
```

```
IPv6 config>set ca
number of cache entries [64]?
```

```
IPv6 config>set mld query-interval
Network interface [0]? 5
New Query Interval (in secs) [125]?
```

```
IPv6 config>set mld response-interval
Network interface [0]? 5
New Response Interval (in secs) [10]?
```

```
IPv6 config>set mld robust
Network interface [0]? 5
New Robustness Variable [2]?
IPv6 config>set mld leave
Network interface [0]?
New Leave Interval (in secs) [1]?
IPv6 config>?
```

access-control

Especifica si el control de acceso está habilitado o inhabilitado.

Valores válidos: on (activo) u off (inactivo)

Valor por omisión: off

automatic-tunnel-parameters

Especifica los valores del parámetro de túnel para los túneles automáticos que fluyen a través del direccionador.

ttl value Especifica el valor del tiempo de vida de las tramas encapsuladas para el túnel.

Valores válidos:

Valor por omisión: 64

allow fragmentation in tunnel?

Especifica si estará permitida la fragmentación en el túnel. Si especifica *yes* estará permitida la fragmentación en el túnel, en el caso de que la red IPv4 que esté usando éste no proporcione la información suficiente para que el dispositivo devuelva un mensaje "Packet Too Big" (Paquete demasiado grande) al sistema principal de IPv6.

Valores válidos: yes o no

Valor por omisión: no

hop count

Especifica la cuenta de saltos que se usará en los paquetes que se ponen en túnel automáticamente.

Valores válidos: De 1 a 255

Valor por omisión: 64

cache-size

Especifica el tamaño de almacenamiento intermedio para la antememoria de la vía de acceso de reenvío rápido.

number of cache entries

Especifica el número de entradas de la antememoria de la vía de acceso de reenvío rápido.

Valores válidos De 64 a 10 000

Valor por omisión: 64

default network-gateway

default gateway

Valores válidos: Cualquier dirección de IPv6 válida

Valor por omisión: ninguno

gateway's cost

Especifica el coste asociado a esta pasarela.

Valores válidos: De 1 a 255

Valor por omisión: 1

default subnet-gateway

for which subnetted network

Valores válidos: Cualquier dirección de IPv6 válida

Valor por omisión: ninguno

default gateway

Valores válidos: Cualquier dirección de IPv6 válida

Valor por omisión: ninguno

gateway's cost

Especifica el coste asociado a esta pasarela.

Valores válidos: De 1 a 255

Valor por omisión: 1

internal-ip-address

Valores válidos: Cualquier dirección de IPv6 válida

Valor por omisión: Ninguno

mld

query-interval

network interface

Valores válidos: Cualquier número de interfaz de red válido

Valor por omisión: 0

Mandatos de configuración de IPv6 (Talk 6)

new query interval (in secs)

Valores válidos: De 1 a 3600

Valor por omisión: 125

response-interval

network interface

Valores válidos: Cualquier número de interfaz de red válido

Valor por omisión: 0

new response interval (in secs)

Valores válidos: De 1 a 60

Valor por omisión: 10

robustness-variable

network interface

Valores válidos: Cualquier número de interfaz de red válido

Valor por omisión: 0

new robustness variable

Valores válidos: De 2 a 10

Valor por omisión: 2

leave-interval

network interface

Valores válidos: Cualquier número de interfaz de red válido

Valor por omisión: 0

new leave interval (in secs)

Valores válidos: De 1 a 60

Valor por omisión: 1

path-mtu-aging-timer

Especifica la antigüedad, en minutos, de las MTU de las vías de acceso determinadas usando path MTU discovery.

Valores válidos: De 10 a 60 minutos, donde 0 = inhabilitar

Valor por omisión: 10

reassembly-size

Especifica el tamaño del ensamblaje de almacenamientos intermedios usados para procesar la cabecera del fragmento.

Valores válidos: De 2048 a 65536

Valor por omisión: 12000

router-id Especifica la dirección de IPv6 del direccionador.

Valores válidos: Cualquier dirección de IPv6 válida

Valor por omisión: Ninguno

routing table-size**number of nets**

Valores válidos: De 64 a 65 535

Valor por omisión: 768

ttl Especifica el valor del tiempo de vida de IPv6.

Valores válidos:

Valor por omisión: 64

Update

Use el mandato **update** para actualizar el filtro de paquetes

Sintaxis:

update packet-filter

packet-filter

Use este mandato para acceder al indicador del mandato Packet-filter 'xx' Config> desde el que puede configurar filtros de paquetes.

Mandatos de actualización del filtro de paquetes

<i>Tabla 114. Resumen de los mandatos de configuración del filtro de paquetes</i>	
Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte la sección "Cómo obtener ayuda" en la página xxix.
Add	Añade control de acceso.
Change	Cambia el control de acceso.
Delete	Suprime un control de acceso.
Move	Reordena la lista de control de acceso aplicada al filtro de paquetes.
List	
Exit	Le devuelve al nivel de mandatos anterior. Consulte la sección "Cómo salir de un entorno de nivel inferior" en la página xxix.

Add

Use el mandato **update packet-filter add** para añadir una lista de control de accesos.

Sintaxis:

add *access-control tipo dirorigen prefijorigen dirdest prefijodest*

access-control

Añade un elemento de control de acceso a la lista de control de acceso.

Type Especifica si el control de acceso es incluyente o excluyente.

Valores válidos: I o E

Valor por omisión: I

Internet source

Especifica la dirección de IPv6 del origen del paquete.

Valores válidos: Cualquier dirección de IPv6 válida

Valor por omisión: Ninguno

Prefix length

Valor decimal que especifica cuántos bits contiguos situados más a la izquierda de la dirección de IPv6 forman el prefijo.

Valores válidos: De 0 a 128

Valor por omisión: 128

Internet destination

Especifica la dirección de IPv6 del destino del paquete.

Valores válidos: Cualquier dirección de IPv6 válida

Valor por omisión: Ninguno

Prefix length

Valor decimal que especifica cuántos bits contiguos situados más a la izquierda de la dirección de IPv6 forman el prefijo.

Valores válidos: De 0 a 128

Valor por omisión: 128

Starting protocol number

Especifica el número de protocolo de inicio de un rango de números de protocolo. Entre un 0 para seleccionar todos los protocolos.

Algunos números de protocolo comunes son:

1 para ICMP

6 para TCP

17 para UDP

89 para OSPF

50 para ESP-Encryption

51 para AH-Encryption

Valores válidos: de 0 a 255

Valores por omisión: 0

Ending protocol number

Especifica el número de protocolo final de un rango de números de protocolo. Entre un 0 para seleccionar todos los protocolos.

Algunos números de protocolo comunes son:

- 1 para ICMP
- 6 para TCP
- 17 para UDP
- 89 para OSPF
- 50 para ESP-Encryption
- 51 para AH-Encryption

Valores válidos: de 0 a 255

Valores por omisión: el valor especificado en el parámetro **starting protocol number**

Starting destination port number

Especifica el número del puerto de inicio de un rango de números de puerto de destino TCP/UDP. Estos parámetros sólo son válidos si el rango de números de protocolo incluye 6 (para TCP) o 17 (para UDP). No se tendrán en cuenta estos parámetros para los paquetes en los cuales el número de protocolo no sea 6 ó 17.

Algunos números de puerto usados normalmente son:

- 21 para FTP
- 23 para Telnet
- 25 para SMTP
- 513 para rlogin
- 520 para RIP

Valores válidos: De 0 a 65535

Valor por omisión: 0

Ending destination port number

Especifica el número del puerto final de un rango de números de puerto de destino TCP/UDP. Estos parámetros sólo son válidos si el rango de números de protocolo incluye 6 (para TCP) o 17 (para UDP). No se tendrán en cuenta estos parámetros para los paquetes en los cuales el número de protocolo no sea 6 ó 17.

Algunos números de puerto usados normalmente son:

- 21 para FTP
- 23 para Telnet
- 25 para SMTP
- 513 para rlogin
- 520 para RIP

Valores válidos: De 0 a 65535

Valor por omisión: el valor especificado como **starting destination port number**

Starting source port number

Especifica el número del puerto de inicio de un rango de números de puerto de origen TCP/UDP. Estos parámetros sólo son válidos si el rango de números de protocolo incluye 6 (para TCP) o 17 (para UDP). No se tendrán en cuenta estos parámetros para los paquetes en los cuales el número de protocolo no sea 6 ó 17. Consulte la descripción de **starting destination port number** para obtener una lista de los números de puerto TCP/UDP más usados.

Valores válidos: De 0 a 65535

Valor por omisión: 0

Ending source port number

Especifica el número del puerto final de un rango de números de puerto de origen TCP/UDP. Estos parámetros sólo son válidos si el rango de números de protocolo incluye 6 (para TCP) o 17 (para UDP). No se tendrán en cuenta estos parámetros para los paquetes en los cuales el número de protocolo no sea 6 ó 17. Consulte la descripción de **starting destination port number** para obtener una lista de los números de puerto TCP/UDP más usados.

Valores válidos: De 0 a 65535

Valor por omisión: el valor especificado como **starting source port number**

Change

Use el mandato **update packet-filter change** para cambiar el control de acceso.

Sintaxis:

change *access-control tipo dirorigen prefijorigen dirdest prefijodest*

access-control

Cambia un elemento del control de acceso.

Type Especifica si el elemento del control de acceso es incluyente o se usa para identificar paquetes a asegurar.

Valores válidos: I o S

Valor por omisión: I

Internet source

Especifica la dirección de IPv6 del origen del paquete.

Valores válidos: Cualquier dirección de IPv6 válida

Valor por omisión: Ninguno

Prefix length

Valor decimal que especifica cuántos bits contiguos situados más a la izquierda de la dirección de IPv6 forman el prefijo.

Valores válidos: De 0 a 128

Valor por omisión: 128

Internet destination

Especifica la dirección de IPv6 del destino del paquete.

Valores válidos: Cualquier dirección de IPv6 válida

Valor por omisión: Ninguno

Prefix length

Valor decimal que especifica cuántos bits contiguos situados más a la izquierda de la dirección de IPv6 forman el prefijo.

Valores válidos: De 0 a 128

Valor por omisión: 128

Delete

Use el mandato **update packet-filter delete** para eliminar un elemento de control de acceso de la lista de control de acceso.

Sintaxis:

delete *access-control* *núm.índice*

access-control

Suprime un control de acceso.

index of access control to be deleted

Especifica el índice de la configuración del control de acceso a eliminar.

Valores válidos: 1 para el número de registros de control de acceso definidos para este filtro de paquetes

Valor por omisión: 1

Move

Use el mandato **update packet-filter move** para volver a ordenar la lista de control de acceso aplicada al filtro de paquetes.

Sintaxis:

move *access-control* *núm.índice despuésnúm.*

access-control

index of control to move

Valores válidos: 1 para el número de registros de control de acceso definidos para este filtro de paquetes

Valor por omisión: 1

Move record after record number

Especifica la ubicación de destino en la lista de control de acceso. Se le solicitará que verifique que se trata de la acción que desea configurar.

Valores válidos: 1 para el número de registros de control de acceso definidos para este filtro de paquetes

Valor por omisión: 0

Mandatos de supervisión de IPv6 (Talk 5)

List

Use el mandato **update packet-filter list** para visualizar la configuración de la lista de control de acceso.

Sintaxis:

```
list          access-controls
```

Ejemplo:

```
Packet-filter 'x' Config> li acc
Access control is : enabled
List of access control records:

1  Type=IS  Source=2001:1::6101/128
    Dest= 2001:1::86/128
    Tid=3

2  Type=I   Source=::/0
    Dest=::/0

Packet-filter 'x' Config>
```

Acceso al entorno de supervisión de IPv6

Siga el procedimiento siguiente para acceder a los mandatos de configuración de IPv6. Este proceso le dará acceso al proceso de supervisión de IPv6.

1. En el indicador OPCON, entre **talk 5**. (Para obtener información más detallada sobre este mandato, consulte el capítulo titulado “The OPCON Process and Commands” (Los mandatos y el proceso OPCON) en el manual *Software User's Guide*.) Por ejemplo:

```
* talk 5
+
```

Después de entrar el mandato **talk 5**, el indicador de GWCON (+) aparecerá en el terminal. Si el indicador no aparece cuando entre por primera vez la configuración, pulse de nuevo **Retorno**.

2. En el indicador +, entre el mandato **p ipv6** para obtener el indicador ipv6>.

Ejemplo:

```
+ p ipv6
ipv6>
```

Mandatos de supervisión de IPv6

Esta sección describe los mandatos de supervisión de IPv6.

Tabla 115 (Página 1 de 2). Resumen de los mandatos de supervisión de IPv6

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte la sección “Cómo obtener ayuda” en la página xxix.
access-control	Muestra los registros de control de acceso.

Tabla 115 (Página 2 de 2). Resumen de los mandatos de supervisión de IPv6

Mandato	Función
cache	Muestra las entradas de la antememoria.
counters	Visualiza los contadores
dump routing tables	Vuelca las tablas de direccionamiento configuradas.
interface addresses	Muestra las direcciones definidas en la interfaz.
internal address	Muestra la dirección interna especificada.
mcast	Muestra una lista de las direcciones de difusión múltiple registradas.
mld	Muestra los parámetros o contadores de MLD.
reset	Restablece la interfaz de IPv6.
route	
sizes	Muestra los tamaños de los almacenamientos intermedios.
sniffer	Establece diversas opciones de rastreo.
static routes	Muestra rutas estáticas.
packet- filter	Muestra filtros de paquetes configurados.
path-mtu	
ping6	Activa el Ping.
traceroute6	Rastrea dinámicamente una ruta.
tunnels	Muestra los túneles configurados.
Exit	Le devuelve al nivel de mandatos anterior. Consulte la sección "Cómo salir de un entorno de nivel inferior" en la página xxix.

Access-control

Use el mandato **access-control** para supervisar los registros de control de acceso configurados.

Sintaxis:

access-control

Cache

Use el mandato **cache** para visualizar.

Sintaxis:

cache

Ejemplo:

```
IPv6>cache
Destination                               Usage           Next hop
```

Counters

Use el mandato **counters** para visualizar el estado de los contadores.

Sintaxis:

counters

Ejemplo:

```
IPv6>counters
Routing errors
Count  Type
      0  Routing table overflow
      0  Net unreachable
      0  Bad subnet number
      0  Bad net number
      0  Unhandled broadcast
      0  Unhandled anycast
      0  Unhandled directed broadcast
      0  Attempted forward of LL broadcast
0
      0  None

Packets discarded through filter 0
IP multicasts accepted:          0

IP input packet overflows
Net  Count
ATM/0 0
NHRPL/0 0
TKR/0 0
TKR/1 0
FR/0 0
PPP/0 0
IP64/0 0
```

Vuelco de tablas de direccionamiento

Use el mandato **dump** para visualizar las tablas de direccionamiento configuradas.

Sintaxis:

dump

Ejemplo:

```
IPv6>dump
Type  Dest net/Prefix          Cost  Age  Next hop(s)
Stat* 1:2:3:4:5:6:7:8/128      100  30   IP64/0

IPv6 Routing table size: 768 nets (79872 bytes), 1 nets known
                        0 nets hidden, 0 nets deleted, 0 nets inactive
                        0 routes used internally, 767 routes free
```

Direcciones de interfaz

Use el mandato **interface** para visualizar las direcciones configuradas en la interfaz.

Sintaxis:

interface

Ejemplo:IPv6>**interface**

Interface	Net:Status	IPV6 State	IPV6 MTU	ICMP redir	IPV6 Address/Prefixlen
Eth/0	0 : DWN	DWN	1500	Enabled	2003:6:14:1::610/64
Eth/1	1 : DWN	DWN	1500	Enabled	2003:7:6:1::610/64
IP64/0	3 : UP	UP	2048	Enabled	FE80::14FF:FE80:3/64

Dirección interna

Use el mandato **internal** para visualizar la dirección interna especificada.

Sintaxis:internal**Mcast**

Use el mandato **mcast** para visualizar las direcciones de difusión múltiple configuradas.

Sintaxis:mcast**Ejemplo:**IPv6>**mcast**

List of IPV6 registered multicast addresses

Interface: Eth/0:

```

Address/Ref_Cnt
FF02::1/1
FF02::2/1
FF02::1:FF00:610/1
FF02::1:FF02:6200/1
FF02::9/1

```

Mld

Use el mandato **mld** para visualizar lo configurado.

Sintaxis:

```

mld                counters
                    parameters

```

Ejemplo:

Mandatos de supervisión de IPv6 (Talk 5)

```
IPv6>m1d counters
Net      Querier      Polls Sent      Polls Rcvd      Reports Rcvd
----      -
IPv6>m1d parameters
Net      Robustness    Query Interval  Response Interval  Leave Query Interval
      Variable    (secs)          (secs)             (secs)
----      -
IPv6>
```

Reset

Use el mandato **reset** para restablecer dinámicamente la interfaz IPv6.

Sintaxis:

```
reset          ipv6
```

Ejemplo:

```
IPv6>reset ipv6
```

Route

Use el mandato **route** para mostrar la ruta a la dirección de IPv6.

Sintaxis:

```
route          dirección
```

Ejemplo:

```
IPv6>route 6::9
IPv6>
```

Sizes

Use el mandato **sizes** para visualizar los tamaños de los almacenamientos intermedios configurados.

Sintaxis:

```
sizes
```

Ejemplo:

```
IPv6>sizes
Routing table size:          768
Table entries used:         3
Reassembly buffer size:    12000
Largest reassembled pkt:    0
Size of routing cache:      64
# cache entries in use:     0
IPv6>
```


Path-mtu

Use el mandato **path-mtu** para mostrar las vías de acceso identificadas como poseedoras de una MTU inferior al tamaño de un paquete enviado por la vía de acceso.

Sintaxis:

`path-mtu`

Ejemplo:

Ping6

Use el mandato **ping6** para ejecutar un ping a una dirección de IPv6.

Sintaxis:

`ping6`

Ejemplo:

```
IPv6>ping
Destination IPv6 address [::]? 8::9
Source IPv6 Address [1::8]?
Ping data size in bytes [56]?
Ping TTL [64]?
Ping rate in seconds [1]?
PING6 1::8 -> 8::9: 56 data bytes, ttl=64, every 1 sec.
```

```
----8::9 PING6 Statistics----
36 packets transmitted, 36 packets received
```

Destination IPv6 address

Valores válidos: Cualquier dirección de IPv6 válida

Valor por omisión: Ninguno

Source IPv6 address

Valores válidos: Cualquier dirección de IPv6 válida

Valor por omisión: Ninguno

Ping data size in bytes

Valores válidos: De 0 al tamaño del almacenamiento intermedio global

Valor por omisión: 56

Ping ttl Especifica el tiempo de vida restante del ping.

Valores válidos: De 1 a 255

Valor por omisión: 64

Ping rate in seconds

Especifica la frecuencia del ping.

Valores válidos: De 1 a 60

Valor por omisión: 1

Traceroute6

Use el mandato **traceroute6** para rastrear dinámicamente una ruta.

Sintaxis:

traceroute6 ...

Ejemplo:

```
IPv6>traceroute6
Destination IPv6 address []? 7::8
Source IPv6 address []? 6::9
Data size in bytes [56]?
Number of probes per hop [3]?
Wait time between retries in seconds [3]?
Maximum TTL [32]?
TRACEROUTE6 7::8: 56 data bytes
 1 * * * *
IPv6>
```

Destination IPv6 address

Valores válidos: Cualquier dirección de IPv6 válida

Valor por omisión: Ninguno

Source IPv6 address

Valores válidos: Cualquier dirección de IPv6 válida

Valor por omisión: Ninguno

Data size in bytes

Valores válidos: De 0 al tamaño del almacenamiento intermedio global

Valor por omisión: 56

Number of probes per hop

Valores válidos: De 1 a 10

Valor por omisión: 3

Wait time between retries in seconds

Valores válidos: De 1 a 60

Valor por omisión: 3

Maximum ttl

Valores válidos: De 1 a 255

Valor por omisión: 32

Tunnels

Use el mandato **tunnels** para visualizar los túneles configurados.

Sintaxis:

tunnels

Ejemplo:

```
IPv6>tunnels
          Configured Tunnels
Tun#  Remote Endpoint  Local Endpoint  Frag Allowed  TTL  MTU  Net#  IPv6 Address/Prefix
  1    1.2.3.4           2.3.4.5        No            100  2048  7     1:2:3:4:5:6:7:8/128

          Automatic Tunnels
Tun#  Remote Endpoint  Frag Allowed  TTL  MTU
IPv6>
```

Soporte de reconfiguración dinámica de IPv6

Esta sección describe la reconfiguración dinámica (DR) en la medida en que afecta a los mandatos de Talk 6 y Talk 5.

Delete Interface de CONFIG (Talk 6)(Suprimir interfaz)

IP Version 6 (IPv6) da soporte al mandato de CONFIG (Talk 6) **delete interface** sin ninguna restricción.

Activate Interface de GWCON (Talk 5)(Activar interfaz)

IPv6 da soporte al mandato de GWCON (Talk 5) **activate interface**, teniendo en cuenta lo siguiente:

Si IPv6 no se ha configurado antes, es necesario rearrancar.

Todos los mandatos específicos de la interfaz de IPv6 están soportados por el mandato de GWCON (Talk 5) **activate interface**.

Reset Interface de GWCON (Talk 5)(Restablecer interfaz)

IPv6 da soporte al mandato de GWCON (Talk 5) **reset interface**, teniendo en cuenta lo siguiente:

- Si IPv6 no se ha configurado antes, es necesario rearrancar.
- Si la asignación de memoria es anómala, es necesario rearrancar.

Todos los mandatos específicos de la interfaz de IPv6 están soportados por el mandato de GWCON (Talk 5) **reset interface**.

Mandatos Component Reset de GWCON (Talk 5)(Restablecer componente)

IPv6 da soporte a los siguientes mandatos **reset** de GWCON (Talk 5) específicos de IPv6:

Mandato GWCON, Protocol IPv6, Reset IPv6

Descripción: Vuelve a leer la SRAM y reinicializa IPv6. También restablece RIP6, NDP6 y PIM6.

Efecto en la red: Ninguno.

Limitaciones: Ninguna.

Todos los cambios de configuración de IPv6 se activan automáticamente excepto los siguientes:

Mandatos cuyos cambios no se activan con el mandato GWCON, protocolo ipv6, reset ipv6
CONFIG, protocol ipv6, set routing table-size
CONFIG, protocol ipv6, set reassembly-size
CONFIG, protocol ipv6, set cache-size

Mandatos Immediate Change de CONFIG (Talk 6)(Cambio inmediato)

IPv6 da soporte a los siguientes mandatos de CONFIG que cambian inmediatamente el estado operativo del dispositivo. Estos cambios se guardan y se conservan si se vuelve a cargar o se reinicia el dispositivo, o si se ejecuta un mandato reconfigurable dinámicamente.

Mandatos
CONFIG, protocol ipv6, add route
CONFIG, protocol ipv6, delete route
CONFIG, protocol ipv6, change route
CONFIG, protocol ipv6, enable icmp-redirect
CONFIG, protocol ipv6, disable icmp-redirect
CONFIG, protocol ipv6, set access-control
CONFIG, protocol ipv6, set ttl
CONFIG, protocol ipv6, set path-mtu-aging-timer

Configuración y supervisión de Neighbor Discovery Protocol (NDP)

En cada interfaz se configura NDP. Este capítulo describe cómo usar los mandatos de funcionamiento y de configuración de NDP e incluye las secciones siguientes:

- “Acceso al entorno de configuración de NDP”
- “Mandatos de configuración de NDP”
- “Acceso al entorno de supervisión de NDP” en la página 513
- “Mandatos de supervisión de NDP” en la página 514
- “Soporte de reconfiguración dinámica de NDP6” en la página 515

Acceso al entorno de configuración de NDP

Siga el procedimiento siguiente para acceder al proceso de configuración de NDP.

1. En el indicador OPCON, entre **talk 6**. (Para obtener información detallada sobre este mandato, consulte *The OPCON Process and Commands* en el manual Guía del usuario de software.) Por ejemplo:

```
* talk 6
Config>
```

Después de entrar el mandato **talk 6**, el indicador CONFIG (Config>) aparecerá en el terminal. Si el indicador no aparece cuando entre por primera vez la configuración, pulse **Intro** de nuevo.

2. En el indicador CONFIG, entre el mandato **p ndp** para obtener el indicador NDP6 Config>.

Mandatos de configuración de NDP

Para configurar NDP, entre los mandatos en el indicador NDP6 Config>.

Tabla 116. Resumen de mandatos de configuración de NDP

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte la sección “Cómo obtener ayuda” en la página xxix.
add	Añade un anuncio de direccionador o parámetros.
change	Cambia un anuncio de direccionador o parámetros.
delete	Suprime un anuncio de direccionador o parámetros.
disable	Inhabilita el anuncio del direccionador.
enable	Habilita el anuncio del direccionador.
list	Lista la configuración.
set	Establece la cuenta de saltos de DHCP.
Exit	Le devuelve al nivel de mandatos anterior. Consulte la sección “Cómo salir de un entorno de nivel inferior” en la página xxix.

Add

Use el mandato **add** para añadir un anuncio de direccionador.

add ra ...
 dhcp-server

ra Añade un anuncio de direccionador.

add router advertisement on which interface

Especifica la interfaz a la que se añadirá el anuncio del direccionador.

Valores válidos: Un valor numérico que identifique una interfaz de red

Valor por omisión: 0

Managed address configuration (stateful)

Especifica si los sistemas principales usan el protocolo administrado para la configuración automática de direcciones además de las direcciones configuradas automáticamente con la configuración automática sin estado.

Valores válidos: yes (sí) o no

Valor por omisión: no

Si especifica *yes*, el agente de retardo de DHCPv6 permitirá que los sistemas principales usen direcciones de enlace locales en el momento de la configuración de direcciones, incluso aunque el servidor DHCPv6 no esté en el mismo enlace.

Other stateful configuration

Especifica si los sistemas principales usan el protocolo administrado para la configuración automática de otra información (no de direcciones).

Valores válidos: yes (sí) o no

Valor por omisión: no

Include link layer address with router advertisement

Especifica si se ha de incluir la dirección de la capa de enlace en el anuncio del direccionador. Un direccionador puede omitir la dirección de la capa del enlace en el anuncio del direccionador para habilitar la compartición de carga de entrada por varias direcciones de capas de enlace.

Valores válidos: yes (sí) o no

Valor por omisión: yes

Hop limit Especifica el valor por omisión que se pondrá en el campo de límite de saltos de los mensajes de anuncio que el direccionador envía. Este valor se usa en el campo de cuenta de saltos de la cabecera IP para los paquetes IP de salida.

Valores válidos: De 0 a 255, donde 0 significa que este direccionador no especifica

Valor por omisión: 0

Maximum router advertisement interval

Especifica el tiempo máximo, en segundos, permitido entre el envío de anuncios del direccionador en difusión múltiple y sin solicitar, desde la interfaz.

Valores válidos: De 4 a 1800 segundos

Valor por omisión: 600

Minimum router advertisement interval

Especifica el tiempo mínimo, en segundos, permitido entre el envío de anuncios del direccionador en difusión múltiple y sin solicitar, desde la interfaz.

Valores válidos: De 3 a $(.75 * \textit{Maximum router advertisement interval})$

Valor por omisión: $\textit{Maximum router advertisement interval}/3$

Router lifetime

Especifica el tiempo, en segundos, durante el cual se usará el direccionador como direccionador por omisión.

Valores válidos: De 0 ó 4 a 9000 segundos, donde 0 indica que el direccionador no se usa como direccionador por omisión

Valor por omisión: $(3 * \textit{Maximum router advertisement interval})$

Reachable Time

Especifica el tiempo, en segundos, en que un nodo asume que un vecino es accesible, después de haber recibido confirmación de accesibilidad.

Valores válidos: De 0 a 3600 segundos, donde el 0 indica sin especificar por este direccionador

Valor por omisión: 0

Retransmit timer

Especifica el tiempo, en segundos, entre los mensajes de solicitud de vecino retransmitidos.

Valores válidos: De 0 a 3600 segundos, donde el 0 indica sin especificar por este direccionador

Valor por omisión: 0

link-mtu

Especifica el valor que se pondrá en las opciones de MTU enviadas por el direccionador. Este valor debe enviarse a enlaces que tienen una MTU variable y puede enviarse a otros enlaces.

Valores válidos: Un entero de 32 bits sin signo, donde el 0 indica que no se envía ninguna opción de MTU

Valor por omisión: 0

dhcp-server

Añade un servidor DHCP.

server addresses

Especifica una lista de direcciones de difusión individual del servidor de IPv6 que se usarán para reenviar el mensaje de solicitud DHCPv6 inicial. Si no se especifica ninguna dirección, el agente de relé DHCPv6 envía el paquete a las direcciones de difusión múltiple de los servidores de DHCP.

Nota: Si usa la dirección de servidores de difusión múltiple, deberá habilitar el direccionamiento de difusión múltiple en la caja habilitando y configurando Protocol Independent Multicast (PIM). Consulte “Configuración y supervisión de Protocol Independent Multicast Routing Protocol (PIM)” en la página 517 para obtener más información.

Valores válidos: Cualquier dirección de IPv6 válida

Valor por omisión: Ninguno

Change

Use el mandato **change** para cambiar un anuncio de ruta o un prefijo.

Sintaxis:

```
change          ...prefix ...  
ra
```

prefix Cambia un prefijo configurado. Los prefijos se añaden y se suprimen a medida que modifica la configuración de la dirección de IPv6. Consulte “Add” en la página 476 para obtener más información sobre cómo añadir direcciones de IPv6.

Para añadir un prefijo:

```
Config> p IPv6  
IPv6 user configuration  
IPv6 config> add addr  
Which net is this address for [0]? 5  
New address []? 2002:9::6204  
Prefix length must be between 8 and 128 [128]? 64  
IPv6 config> exit
```

Para cambiar un prefijo:

```
Config> p ndp6  
Neighbor Discovery for IPv6 user configuration  
NDP6 Config> change prefix  
Change Prefix Information option for which Prefix address []? 2002:2::  
Use this prefix for on-link determination? [Yes]:  
Use this prefix for autonomous address configuration? [Yes]: n  
Valid lifetime for Prefix [2592000]? ffffff  
Decrement the Valid Lifetime in real time? [No]:  
Preferred Lifetime for Prefix [604800]? ffffff  
Decrement the Preferred Lifetime in real time? [No]:
```

Change prefix information options for which prefix address?

Especifica el prefijo de la dirección de IPv6 que se pondrá en la opción de información del prefijo, en los anuncios del direccionador enviados desde la interfaz.

Valores válidos: Cualquier dirección de IPv6 válida

Valor por omisión: Ninguno

Use this prefix for on-link determination?

Especifica el valor que se pondrá en el indicador de dentro del enlace en la opción de información del prefijo. Cuando se establece en *yes* (sí), puede usarse el prefijo para la determinación de dentro del enlace. Cuando se establece en *no*, el anuncio no indicará nada sobre las propiedades de dentro del enlace y de fuera del enlace, del prefijo.

Valores válidos: yes (sí) o no

Valor por omisión: yes

Use this prefix for autonomous address configuration?

Especifica el valor que se pondrá en el indicador de configuración de la dirección autónoma, dentro de la opción de información del prefijo. Cuando se establece en *yes* (sí), puede usarse el prefijo para la configuración autónoma de la dirección.

Valores válidos: yes (sí) o no

Valor por omisión: yes

Valid Lifetime for Prefix?

Especifica la cantidad de tiempo, en segundos, que se pondrá en el tiempo de vida válido, dentro de la opción de información del prefijo. Este valor representa el período de tiempo, relativo a la hora de envío del paquete, durante el cual el prefijo será válido para la determinación dentro del enlace.

Valores válidos: Un entero sin signo de 32 bits, donde X'FFFFFFFF' representa un tiempo de vida sin límite

Valor por omisión: 259200 (que corresponde a 30 días)

Decrement the Valid Lifetime in real time?

Especifica si el Valid Lifetime (tiempo de vida válido) disminuye en tiempo real, con lo que en un futuro, el tiempo de vida llegará a cero en el momento especificado O bien si es fijo (sigue siendo el mismo en los anuncios del direccionador consecutivos).

Valores válidos: yes (sí) o no

Valor por omisión: no

Preferred lifetime for prefix

Especifica la cantidad de tiempo, en segundos, que se pondrá en el tiempo de vida preferido, dentro de la opción de información del prefijo. Este valor representa el período de tiempo, relativo a la hora de envío del paquete, durante el cual las direcciones generadas a partir del prefijo a través de la configuración automática de las direcciones sin estado, siguen siendo preferidas.

Valores válidos: Un entero sin signo de 32 bits, donde X'FFFFFFFF' representa un tiempo de vida sin límite

Valor por omisión: 604800

Mandatos de configuración de NDP (Talk 6)

Decrement the Preferred Lifetime in real time?

Especifica si el Preferred Lifetime (tiempo de vida preferido) disminuye en tiempo real, con lo que en un futuro, el tiempo de vida llegará a cero en el momento especificado o bien si es fijo (sigue siendo el mismo en los anuncios del direccionador consecutivos).

Valores válidos: yes (sí) o no

Valor por omisión: no

ra Cambia un anuncio de una ruta configurada. Consulte “Add” en la página 508 para obtener una descripción de los parámetros asociados al mandato **change ra**.

Delete

Use el mandato **delete** para eliminar un anuncio de ruta configurado.

Sintaxis:

```
delete          dhcp-server  
                ra
```

Disable

Use el mandato **disable** para inhabilitar el anuncio de rutas.

Sintaxis:

```
disable        dhcp-relay  
                ra
```

dhcp-relay

Inhabilita el agente de relé de DHCPv6.

ra Inhabilita el anuncio de ruta.

Enable

Use el mandato **enable** para habilitar el anuncio de ruta.

Sintaxis:

```
enable         dhcp-relay  
                ra
```

dhcp-relay

Habilita el agente de relé de DHCPv6.

ra Habilita el anuncio de ruta.

List

Use el mandato **list** para visualizar la configuración de NDP.

Sintaxis:

```
list           dhcp  
                ndp6 configuration  
                prefix  
                ra
```


Ejemplo:

```
NDP>list dhcp

DHCPv6 Relay Agent
-----
State           Hopcount
DISABLED        4
NDP>

NDP config>list ndp6

NDP config>list ra

NDP config>list prefix
NDP config>
```

Set

Use el mandato **set** para establecer la cuenta de saltos de DHCP.

Sintaxis:

```
set           dhcp-hopcount
```

dhcp-hopcount

Especifica el número de saltos que se usarán al pasar en relé paquetes de DHCPv6.

Valores válidos:

Valor por omisión: 4

Ejemplo:

```
NDP6 Config>set dhcp-hopcount
Hop Count [4]?
NDP6 Config>
```

Acceso al entorno de supervisión de NDP

Siga el procedimiento siguiente para acceder a los mandatos de supervisión de NDP. Este proceso le dará acceso al proceso de supervisión de NDP.

1. En el indicador OPCON, entre **talk 5**. (Para obtener información más detallada sobre este mandato, consulte "The OPCON Process and Commands" (Los mandatos y el proceso de OPCON) en *Guía del usuario de software*.) Por ejemplo:

```
* talk 5
+
```

Después de entrar el mandato **talk 5**, el indicador de GWCON (+) aparecerá en el terminal. Si el indicador no aparece cuando entre por primera vez la configuración, pulse **Intro** de nuevo.

2. En el indicador +, entre el mandato **p ndp** para obtener el indicador NDP>.

Ejemplo:

```
+ p ndp
NDP>
```

Mandatos de supervisión de NDP

Esta sección describe los mandatos de supervisión de NDP.

Tabla 117. Resumen de los mandatos de supervisión de NDP

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte la sección “Cómo obtener ayuda” en la página xxix.
dhcpv6-relay	Establece los contadores y parámetros de relé de DHCPv6.
dump	Muestra las tablas de direccionamiento.
list	Muestra la configuración.
ping6	Ejecuta ping dinámicos en una dirección de IPv6.
Exit	Le devuelve al nivel de mandatos anterior. Consulte la sección “Cómo salir de un entorno de nivel inferior” en la página xxix.

DHCPv6-Relay

Use el mandato **dhcpv6-relay** para establecer los parámetros y los contadores de relé de DHCPv6.

Sintaxis:

```
dhcpv6-relay    counters  
                  parameters
```

counters

parameters

Ejemplo:

Dump

Consulte “Dump routing tables” en la página 524 para obtener información sobre el mandato **dump**.

List

Use el mandato **list** para visualizar la configuración. Sólo se mostrarán las interfaces que tengan configurado RA, incluso aunque pueda existir un prefijo en la lista de prefijos de otras interfaces, como consecuencia de la configuración de dirección de IPv6.

Sintaxis:

```
list            dhcpv6-relay  
                  dump routing tables  
                  ndp6 parameters  
                  ping6
```

Ejemplo:

```

NDP>list dhcp

DHCPv6 Relay Agent
-----
State           Hopcount
DISABLED        4
NDP>
NDP>list ndp6

Router Advertisement for Interface 0 (PPP/0):

State      M  O  LLA  Limit  Hop  RA Interval  Rtr  Reach  Retrans  MTU
ENABLED    N  N  Y  0      200 - 600  1800  0      0      0

```

Advertised Prefixes: _____ On-Link Auto Valid/Preferred Life

Ping6

Consulte “Ping6” en la página 502 para obtener detalles sobre el mandato **ping6**.

Soporte de reconfiguración dinámica de NDP6

Esta sección describe la reconfiguración dinámica (DR) en la medida en que afecta a los mandatos de Talk 6 y Talk 5.

Delete Interface de CONFIG (Talk 6)(Suprimir interfaz)

Neighbor Discovery Protocol para IPv6 (NDP6) da soporte al mandato de CONFIG (Talk 6) **delete interface** sin ninguna restricción.

Activate Interface de GWCON (Talk 5)(Activar interfaz)

NDP6 da soporte al mandato de GWCON (Talk 5) **activate interface** sin ninguna restricción.

La tabla siguiente resume los cambios de configuración de NDP6 que se activan cuando se invoca el mandato de GWCON (Talk 5) **activate interface**:

Mandatos cuyos cambios se activan con el mandato de GWCON (Talk 5) activate interface
CONFIG, protocol NDP6, add ra
CONFIG, protocol NDP6, change prefix
CONFIG, protocol NDP6, change ra
CONFIG, protocol NDP6, delete ra
CONFIG, protocol NDP6, disable ra
CONFIG, protocol NDP6, enable ra

Reset Interface de GWCON (Talk 5)(Restablecer interfaz)

NDP6 da soporte al mandato de GWCON (Talk 5) **reset interface** sin ninguna restricción.

La tabla siguiente resume los cambios de configuración de NDP6 que se activan cuando se invoca el mandato de GWCON (Talk 5) **reset interface**:

Mandatos cuyos cambios se activan con el mandato de GWCON (Talk 5) reset interface
CONFIG, protocol NDP6, add ra
CONFIG, protocol NDP6, change prefix
CONFIG, protocol NDP6, change ra
CONFIG, protocol NDP6, delete ra
CONFIG, protocol NDP6, disable ra
CONFIG, protocol NDP6, enable ra

Mandatos Component Reset de GWCON (Talk 5)(Restablecer componente)

NDP6 da soporte a los siguientes mandatos de GWCON (Talk 5) **reset** específicos de NDP6:

Mandato GWCON, Protocol IPV6, Reset IPV6

Descripción: Restablece dinámicamente todos los parámetros de configuración de NDP6. Consulte la descripción del mandato bajo IPv6 si desea ver más detalles de este mandato.

Efecto en la red: No hay ninguna interrupción de la red para NDP6.

Limitaciones: Ninguna.

La tabla siguiente resume los cambios de configuración de NDP6 que se activan cuando se invoca el mandato **GWCON, protocol ipv6, reset ipv6**:

Mandatos cuyos cambios se activan con el mandato GWCON, protocol ipv6, reset ipv6
CONFIG, protocol NDP6, add ra
CONFIG, protocol NDP6, change prefix
CONFIG, protocol NDP6, change ra
CONFIG, protocol NDP6, delete ra
CONFIG, protocol NDP6, disable ra
CONFIG, protocol NDP6, enable ra

Configuración y supervisión de Protocol Independent Multicast Routing Protocol (PIM)

La configuración de PIM se efectúa en cada interfaz. Este capítulo describe cómo usar los mandatos de funcionamiento y configuración de PIM e incluye las secciones siguientes:

- “Uso de PIM”
- “Acceso al entorno de configuración de PIM” en la página 518
- “Mandatos de configuración de PIM” en la página 518
- “Acceso al entorno de supervisión de PIM” en la página 523
- “Mandatos de supervisión de PIM” en la página 524
- “Soporte de reconfiguración dinámica de PIM” en la página 532
- “Soporte de reconfiguración dinámica de PIM para IPv6” en la página 533
- “Soporte de reconfiguración dinámica de Multicast Forwarding Cache” en la página 534
- “Soporte de reconfiguración dinámica de Multicast Forwarding Cache V6” en la página 535

Uso de PIM

Protocol Independent Multicast en modalidad densa (PIM-DM) es un protocolo de difusión múltiple de poda y difusión usado por IP. Da soporte tanto a IPv4 como a IPv6, y los mandatos y la sintaxis son idénticos para ambas versiones. Funciona bien en redes de campus, donde la anchura de banda es abundante y los usuarios están fuertemente agrupados, no dispersos en una amplia área de redes. PIM usa un enfoque de poda y reenvío para la difusión en difusión múltiple de datagramas y se usa cuando grupos de difusión múltiple están distribuidos densamente por Internet. Asume que todos los sistemas en sentido directo desean recibir datagramas de difusión múltiple y poda hacia atrás las ramas de aquellos que no lo deseen.

PIM-DM es un protocolo de estado suave. Esto significa que los estados de poda, si no se han eliminado mediante otra actividad (como, por ejemplo, injerto o empalme), se eliminan al cabo de un período de tiempo (configurable) y los datos de difusión múltiple se vuelven a difundir a todos los sistemas en sentido directo donde se vuelve a producir la poda.

PIM-DM establece una adyacencia con direccionadores de PIM vecinos intercambiando mensajes Hello con todos los vecinos. Mantiene activa la adyacencia hasta que se agota. Mientras los direccionadores vecinos estén activos y ejecutándose, se enviarán mensajes Hello nuevos para renovar el estado Hello y evitar que la adyacencia se agote. Se puede configurar la frecuencia de envío de los mensajes Hello.

PIM-DM usa la tabla de direccionamientos de difusión individual, sin tener en cuenta qué protocolo de difusión individual es propietario de una entrada, para llevar a cabo el cálculo de reenvío de vía de acceso inversa en un datagrama de difusión múltiple recibido. El reenvío de vía de acceso inversa (RPF) se usa para validar si el datagrama de difusión múltiple recibido llegó a una interfaz válida para la difusión a la dirección de origen contenida en el datagrama de difusión múltiple. Si se trata de una interfaz incorrecta, se descartará el datagrama o se creará una

Mandatos de configuración de PIM (Talk 6)

entrada de difusión múltiple nueva y se difundirá el datagrama de difusión múltiple al resto de las interfaces (aquellas que tengan PIM-DM activo, miembros del sistema principal local y cualquier interfaz que otros protocolos de difusión múltiple hayan añadido). El uso de rutas de difusión individual para realizar RPF para la validación de interfaces de entrada necesita que el direccionamiento de difusión individual sea simétrico.

El injerto también tiene soporte para permitir que los sistemas principales se unan dinámicamente a un grupo. Esto injertará una rama a un árbol de difusión múltiple ya existente y eliminará todos los estados de poda donde sea necesario, para asegurarse de que los sistemas principales que se hayan unido reciban los datagramas de difusión múltiple de grupo solicitados.

Debido a la naturaleza independiente de PIM en relación con los protocolos de direccionamiento de difusión individual y la naturaleza de difusión de PIM-DM, pueden producirse vías de acceso paralelas de origen y reenviarse datos de difusión múltiple duplicados. PIM-DM usa un procedimiento de afirmación para elegir el direccionador de reenvío adecuado cuando esto se produce. Pueden configurarse preferencias en direccionadores que ejecutan diferentes protocolos de direccionamiento de una difusión para resolver qué direccionador se desea que tenga preferencia. Cuando el direccionamiento de una difusión individual sea el mismo, los costes métricos de una difusión individual al origen se usarán para determinar la mejor ruta. Y cuando el resto sea igual, se elegirá el direccionador que tenga la dirección de interfaz IP más grande como reenviador adecuado.

Use el mandato **p pim** en el indicador `Config>` para configurar parámetros de PIM.

Acceso al entorno de configuración de PIM

Siga el procedimiento siguiente para acceder al proceso de configuración de PIM.

1. En el indicador `OPCON`, entre **talk 6**. (Para obtener información más detallada sobre este mandato, consulte “The OPCON Process and Commands” (Los mandatos y el proceso de OPCON) en *Guía del usuario de software*.) Por ejemplo:

```
* talk 6
  Config>
```

Después de entrar el mandato **talk 6**, el indicador `CONFIG (Config>)` aparecerá en el terminal. Si el indicador no aparece cuando entre por primera vez la configuración, pulse de nuevo **Retorno**.

2. Para IPv4, en el indicador `CONFIG`, entre el mandato **p pim** para obtener el indicador `PIM Config>`. Para IPv6, entre el mandato **p pim6** para obtener el indicador `PIM6 Config>`.

Mandatos de configuración de PIM

Para configurar PIM para IPv4, entre los mandatos en el indicador `PIM Config>`. Para IPv6, entre los mandatos en el indicador `PIM6 Config>`.

Tabla 118. Resumen de los mandatos de configuración de PIM

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte la sección “Cómo obtener ayuda” en la página xxix.
delete	Suprime una interfaz de PIM.
disable	Inhabilita PIM en el dispositivo.
enable	Habilita PIM en el dispositivo y establece los valores de configuración por omisión de PIM globales.
list	Lista la configuración.
set	Establece los valores de los parámetros de configuración de PIM.
Exit	Le devuelve al nivel de mandatos anterior. Consulte la sección “Cómo salir de un entorno de nivel inferior” en la página xxix.

Delete

Use el mandato **delete** para eliminar una interfaz de PIM configurada.

Sintaxis:

delete *dirinterfaz*

Interface address

Ejemplo:

```
PIM Config> delete
Interface address []?
```

Disable

Use el mandato **disable** para inhabilitar PIM en el dispositivo.

Sintaxis:

disable

Enable

Use el mandato **enable** para habilitar PIM en el dispositivo y establecer los valores de configuración por omisión de PIM globales.

Sintaxis:

enable

List

Use el mandato **list** para visualizar la configuración de PIM.

Sintaxis:

list *all*
interface
preference
variables

Mandatos de configuración de PIM (Talk 6)

- all** Muestra toda la información de configuración de PIM.
- interface** Muestra la información de configuración de PIM de las interfaces configuradas actualmente.

Ejemplo:

```
PIM Config>list i
```

Type	IP Address	Hello Interval	State Holdtime
Physical	9.37.2.1	30	210

Type Identifica el tipo de interfaz configurada.

IP address

Identifica la dirección de IP asignada a esta interfaz.

Hello Interval

Identifica el intervalo transcurrido entre los mensajes hello, en segundos, enviados en esta interfaz.

State holdtime

Identifica el número de segundos necesarios para indicar a otros dispositivos en sentido inverso que mantengan el estado PIM de este dispositivo. Para PIM, se trata de la cantidad de tiempo necesario para que los dispositivos en sentido inverso mantengan vivas las podas.

- variables** Muestra información de configuración de las variables de PIM globales.

Ejemplo:

```
PIM Config>list v
```

```
PIM Global Configuration Values
```

```
PIM: on
```

```
Graft Timeout: 3 seconds  
Assert Timeout: 210 seconds
```

```
PIM Config>
```

PIM: on/off

Identifica si PIM está habilitado o no actualmente.

Graft timeout

Identifica el número de segundos durante el cual se vuelven a transmitir injertos si no se ha recibido ningún acuse de recibo de injerto.

Assert timeout

Identifica el número de segundos durante el cual la información de validación, obtenida a partir de dispositivos de comunicaciones en sentido inverso, se retiene antes de volver a la información de direccionamiento local.

preference

Muestra las preferencias métricas del tipo de direccionamiento configurado actualmente.

Ejemplo: (sólo IPv4)


```
PIM Config>list p
```

```
Direct    0
Static    1
OSPF      110
RIP       120
BGP       200
```

```
PIM Config>
```

Route type

Identifica el tipo de ruta con soporte y lista un valor hexadecimal mostrando la preferencia métrica configurada actualmente.

Set

Use el mandato **set** para cambiar los valores del parámetro de configuración de PIM. Puede usar este mandato para añadir una interfaz física nueva.

Sintaxis:

```
set          interface dirección interfaz períodohello
               tiempo retención poda unida
               preference tipo ruta valor preferencia
               variables
```

interface

Ejemplo:

```
PIM Config>set interface
Interface address []?
Hello period [30]?
Join Prune Hold Time [210]?
```

Interface address

Valores válidos: Cualquier dirección de IP válida

Valor por omisión: Ninguno

Hello period

Especifica el número de segundos transcurridos entre mensajes hello. En las interfaces de punto a punto, no se tiene en cuenta este valor. Una vez 2210 establece una adyacencia, los mensajes hello quedan silenciados.

Valores válidos: De 1 a 65535

Valor por omisión: 30

Join prune hold time

Controla mensajes para informar al dispositivo de recepción cuánto tiempo (en segundos) deberá mantener el estado activado por el mensaje. Las podas enviadas al dispositivo permanecen activas durante este período de segundos.

Valores válidos: De 1 a 65535

Valor por omisión: 210

preference *tiporuta*

Se trata de una preferencia métrica configurada para usarla en el proceso de validación. Permite al usuario seleccionar selectivamente

Mandatos de configuración de PIM (Talk 6)

qué tipos de rutas de difusión individual de las tablas de reenvío de una difusión individual tienen precedencia sobre otros tipos de ruta. Sólo es de significado local, lo que quiere decir que se usa para este dispositivo y todas sus interfaces activadas PIM conectadas. Puede utilizarse si este direccionador usa varios protocolos de direccionamiento de una difusión individual, los direccionadores adyacentes ejecutan diferentes protocolos de direccionamiento o si se prefieren tipos de ruta como, rutas por omisión, sobre las rutas ya sabidas.

Routetype puede especificar los tipos de rutas siguientes:

- direct (directo)
- static (estático)
- ospf (sólo IPv4)
- rip (sólo IPv4)
- bgp

Ejemplo:

```
PIM Config> set preference rip
RIP Metric Preference [120]?
```

Metric Preference

Este valor se envía a otros direccionadores en el proceso de validación, durante la detección de difusiones múltiples duplicadas y se usa con los costos de métrica de rutas para determinar qué direccionador debe ser el direccionador de reenvío. Todas las preferencias métricas se establecen inicialmente en 0.

Rango: 0 - 65535

Valores por omisión:

direct	0
static	1
ospf	110
rip	120
bgp	200

variables cache_life

Ejemplo:

```
PIM Config>set v cache_life
Mcfwd cache Holdtime [60]
```

Mcfwd cache holdtime

Especifica el tiempo, en segundos, que se le permitirá existir a una entrada de difusión múltiple que no se ha usado para reenviar datagramas de difusión múltiple en la antememoria de reenvío de difusión múltiple antes de eliminarla.

Valores válidos: Un valor numérico superior a 0

Valor por omisión: 60

variables assert_tout

Ejemplo:

```
PIM Config>set v assert_tout
PIM Assert Time Out [210]
```

Assert timeout

Cantidad de tiempo, en segundos, durante el cual los direccionadores en sentido directo guardarán información de validación recibida de dos o varios direccionadores de sentido inverso de validación. La información de validación se usa para asegurarse de que los direccionadores en sentido directo comprendan cuál es el direccionador correcto de sentido inverso, o direccionador de reenvío, a fin de que los mensajes de PIM se envíen al direccionador correcto. Si no se reciben más validaciones antes de que el tiempo de validación se agote, la información de validación se descartará y el direccionador usará información local de las tablas de direccionamiento de una difusión individual, para determinar el direccionador de reenvío de sentido inverso correcto.

Valores válidos: De 1 a 65535

Valor por omisión: 210

variables graft_tout

Ejemplo:

```
PIM Config>set v graft_tout
PIM Graft Time Out [3]
```

Graft time out

Especifica el número de segundos durante el cual, el dispositivo que ha enviado el mensaje de injerto, pero no ha recibido ningún acuse de recibo, esperará antes de enviar otro mensaje.

Valores válidos: De 1 a 65535

Valor por omisión: 3

Acceso al entorno de supervisión de PIM

Siga el procedimiento siguiente para acceder a los mandatos de supervisión de PIM. Este proceso le dará acceso al proceso de supervisión de PIM.

1. En el indicador OPCON, entre **talk 5**. (Para obtener información detallada sobre este mandato, consulte *The OPCON Process and Commands* en la Guía del usuario de software.) Por ejemplo:

```
*
talk 5
+
```

Después de entrar el mandato **talk 5**, el indicador de GWCON (+) aparecerá en el terminal. Si el indicador no aparece cuando entre por primera vez la configuración, pulse de nuevo **Retorno**.

Mandatos de supervisión de PIM (Talk 5)

- Para IPv4, en el indicador +, entre el mandato **p pim** para ir al indicador PIM>.
Para IPv6, en el indicador +, entre el mandato **p pim6** para ir al indicador PIM6>.

Ejemplo:

```
+ p pim
PIM>
```

Mandatos de supervisión de PIM

Esta sección describe los mandatos de supervisión de PIM.

Tabla 119. Resumen de mandatos de supervisión de PIM

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte la sección “Cómo obtener ayuda” en la página xxix.
dump	Muestra las tablas de direccionamiento.
clear	Borra la tabla de difusiones múltiples.
interface	Muestra el estado de la interfaz.
join	Une un grupo de difusiones múltiples.
leave	Deja un grupo de difusiones múltiples.
mcache	Muestra las entradas de antememoria de la tabla de difusiones múltiples activa actualmente.
mgroups	Muestra la pertenencia de grupo de las interfaces conectadas al dispositivo.
mstats	Muestra diversas estadísticas de direccionamiento de difusión múltiple.
neighbor	Muestra información sobre las adyacencias actuales.
pim	Muestra la base de datos de estados de PIM.
summary pim	Muestra un resumen de la base de datos de estados de PIM.
ping	Ejecuta ping dinámicos en una dirección de IPv6.
reset	Restablece dinámicamente el PIM.
traceroute	Rastrea dinámicamente una ruta.
variables	Muestra los valores de configuración de las variables de PIM.
Exit	Le devuelve al nivel de mandatos anterior. Consulte la sección “Cómo salir de un entorno de nivel inferior” en la página xxix.

Dump routing tables

Use el mandato **dump** para visualizar las tablas de direccionamiento configuradas.

Sintaxis:

dump

Si desea ver un ejemplo de la salida de este mandato, vea la descripción del mandato **dump routing table** en la sección IP Monitoring Commands del manual *Consulta de configuración y supervisión de protocolos Volumen 1*.

Clear

Use el mandato **clear** para restablecer la antememoria.

Sintaxis:

clear

Ejemplo:

PIM>**clear**

Mfwd Cache has been cleared!

PIM>

Interface

Use el mandato **interface** para mostrar un resumen de las estadísticas y parámetros relacionados con la interfaz.

Sintaxis:

interface

Ejemplo:

PIM>**interface**

PIM Interface Table

IP Address	Hello		State	
	Interval	Holdtime	Status	Type
9.32.45.1	30	210	up	TKR/0
9.10.32,23	30	210	up	TKR/1

PIM>

IP address

Especifica la dirección IP de la interfaz.

Hello interval

Especifica la cantidad de segundos transcurridos entre los mensajes hello de esta interfaz.

State holdtime

Especifica el número de segundos durante el cual los dispositivos de comunicaciones en sentido inverso mantendrán la información de estado antes de descartarla. En el caso de PIM, se trata del número de segundos durante el cual una poda estará activa en las comunicaciones en sentido inverso.

Status

Especifica el estado actual de la interfaz.

up La interfaz está activada y plenamente operativa, pero no genera las consultas mld.

disabled La interfaz es operativa pero está inhabilitada y el PIM no está activo.

down La interfaz no es operativa.

Join

Use el mandato **join** para unir un grupo de difusión múltiple.

Sintaxis:

join

Ejemplo:

```
PIM>join 224.12.2.2
```

Leave

Use el mandato **leave** para dejar un grupo de difusión múltiple. Esto evita que el dispositivo responda a pings y consultas de SNMP enviadas a la dirección de grupo.

Sintaxis:

leave

Ejemplo:

```
PIM>leave 224.12.2.2
```

Mcache

Use el mandato **mcache** para visualizar la lista de entradas de antememoria de difusión múltiple activas actualmente. Estas entradas se crean a petición, siempre que se recibe el primer datagrama de difusión múltiple coincidente. Existe una entrada de antememoria separada (y, por consiguiente una ruta separada) por cada combinación de red de origen de datagramas y grupo de destino.

Sintaxis:

mcache

Ejemplo:

```
PIM>mcache
```

```
0: TKR/0          1: TKR/1          2: TKR/2
3: IPPN/0         4: BDG/0          5: Internal
```

			Prot	Count	Upstr	Downstream
Source	Destination	Owner	Count	Upst	Downstream	
9.10.12.3	224.12.2.2	PIM	124	0	1, 2	
*10.23.55.2	224.32.4.5	PIM	3	1	1	

```
PIM>
```

Prot Especifica el protocolo propietario de la entrada de la tabla de difusiones múltiples.

Count Muestra el número de paquetes de difusión múltiple recibidos para esta entrada de tabla de difusiones múltiples.

Upstr Muestra la red o el direccionador vecinos de los que debe recibirse el datagrama a fin de reenviarlo.

Downstream

Muestra el número total de interfaces en sentido directo o vecinos a los que se reenviará el datagrama.

Mgroups

Use el mandato **mgroups** para visualizar la pertenencia al grupo de las interfaces conectadas al dispositivo. Sólo se visualizará la pertenencia al grupo de aquellas interfaces en las que el direccionador sea el direccionador designado o el direccionador designado de seguridad.

Sintaxis:

mgroups

Ejemplo:

PIM>mgroups

Group	Local Group Database	Interface	Lifetime (secs)
224.12.2.2	9.32.4.5 (TKR/0)	176	
224.5.5.5	Internal	1	

PIM>

Group Muestra la dirección del grupo tal como se ha informado acerca de la misma (a través de MLD) en una interfaz en particular.

Interface Muestra la dirección de la interfaz a la que se ha indicado la dirección de grupo (a través de MLD). La pertenencia al grupo interno del direccionador se indica mediante un valor *internal* (interno). Para estas entradas, el campo lifetime (ver la descripción que aparece a continuación) indica el número de aplicaciones que han solicitado pertenecer a este grupo determinado.

Lifetime Muestra los segundos que persistirá la entrada si dejan de oírse los Membership Reports (Informes de pertenencia) en la interfaz del grupo determinado.

Mstats

Use el mandato **mstats** para visualizar diversas estadísticas de direccionamiento de difusión múltiple. El mandato indica si el direccionamiento de difusión múltiple está habilitado y si el direccionador es un reenviador entre áreas o de difusión múltiple entre AS.

Sintaxis:

mstats

Ejemplo:

Mandatos de supervisión de PIM (Talk 5)

PIM>mstats

```

MOSPF forwarding:      Disabled
Inter-area forwarding: Disabled
DVMRP forwarding:      Enabled
PIM forwarding:         Disabled

Datagrams received:    10143  Datagrams fwd (multicast): 10219
Datagrams fwd (unicast): 0      Locally delivered:          0
Unreachable source:    0      Unallocated cache entries: 0
Off multicast tree:    0      Unexpected DL multicast:    0
Buffer alloc failure:  0      TTL scoping:                0
Administrative filtering: 235

# DVMRP routing entries: 5 # DVMRP entries freed:      0
# fwd cache alloc:       1 # fwd cache freed:          0
#fwd cache GC:          0 # local group DB alloc:    0
# local group DB free:   0
```

PIM>

Datagrams received

Muestra el número de datagramas de difusión múltiple recibidos por el direccionador.

Datagrams fwd (multicast)

Muestra el número de datagramas que se han reenviado como difusiones múltiples de enlaces de datos (esto incluye las réplicas de paquetes, cuando es necesario, por lo que esta cuenta puede ser superior al número recibido).

Datagrams fwd (unicast)

Muestra el número de datagramas que se han reenviado como difusiones individuales de enlace de datos.

Locally delivered

Muestra el número de datagramas que se han reenviado a aplicaciones internas.

Unreachable source

Muestra una cuenta de los datagramas cuya dirección de origen era inaccesible.

Unallocated cache entries

Muestra una cuenta de los datagramas cuyas entradas de antememoria no se pudieron crear debido a falta de recursos.

Off multicast tree

Muestra una cuenta de los datagramas que no se reenviaron porque no había vecino en sentido inverso o no había interfaces/vecinos en sentido directo, en la entrada de antememoria coincidente.

Unexpected DL multicast

Muestra una cuenta de los datagramas que se recibieron como difusiones individuales de enlaces de datos en las interfaces configuradas para difusión individual de enlace de datos.

Buffer alloc failure

Muestra una cuenta de los datagramas a los que no se pudo replicar debido a falta de almacenamientos intermedios.

TTL scoping

Indica los datagramas que no se reenviaron porque su TTL indicaba que no pudieron acceder nunca a un miembro de grupo.

Administrative filtering

Muestra el número de datagramas que se han descartado debido al filtraje de salida.

#fwd cache alloc

Indica el número de las entradas de antememoria asignadas. El tamaño de antememoria de reenvío actual equivale al número de entradas asignadas (**# fwd cache alloc**) menos el número de entradas de antememoria liberadas (**# fwd cache freed**).

#fwd cache freed

Indica el número de entradas de antememoria liberadas. El tamaño de antememoria de reenvío actual equivale al número de entradas asignadas (**# fwd cache alloc**) menos el número de entradas de antememoria liberadas (**# fwd cache freed**).

#fwd cache GC

Indica el número de entradas de antememoria borradas debido a que no se usaron recientemente y la antememoria se desbordó.

#local group DB alloc

Indica el número de entradas de la base de datos de grupos local asignadas. El número asignado (**# asig BD grupos local**) menos el número liberado (**# DB grupo local libre**) es igual al tamaño actual de la base de datos de grupos local.

#local group DB free

Indica el número de entradas de la base de datos de grupos local liberadas. El número asignado (**# asig BD grupos local**) menos el número liberado (**# DB grupo local libre**) es igual al tamaño actual de la base de datos de grupos local.

Neighbor

Use el mandato **neighbor** para visualizar información sobre dispositivos PIM vecinos y el estado de adyacencia.

Sintaxis:

nneighbor

Ejemplo:

```
PIM>neighbor
PIM Neighbor Listing
```

Neighbor Addr	DR	Last Heard	First Heard	Ifc
9.12.2.2	NO	21	6139	TKR/0
9.25.3.111	YES	29	6204	TKR/1

```
PIM>
```

Neighbor Addr

Identifica si este direccionador ha identificado el vecino como el direccionador designado.

Mandatos de supervisión de PIM (Talk 5)

DR Identifica si este direccionador ha identificado el vecino como el direccionador designado.

Last Heard

El número de segundos desde que se oyó por última vez al vecino.

First Heard

El número total de segundos desde que se estableció por primera vez la adyacencia con este vecino.

Ifc La interfaz en la que se descubrió al vecino.

PIM

Use el mandato **pim** para visualizar la base de datos de estados del PIM.

Sintaxis:

pim

Ejemplo:

```
PIM>pim
                PIM State Database
                -----
Interface  Group          Source          Lifetime (sec)
1  PRUNE  224.12.2.2      9.32.4.128      205
1  PRUNE  224.23.121.4    9.124.23.1      155
```

PIM>

Group La dirección del grupo de destino asociada a la entrada.

Source La dirección de origen del originador del datagrama de difusión múltiple.

Interface El número de la interfaz del PIM y el tipo de estado de éste en la base de datos.

Lifetime El tiempo de vida total, en segundos, del estado recibido, obtenido a partir del mensaje de control de PIM que estableció el estado.

Summary PIM

Use el mandato **summary pim** para visualizar información resumida sobre la base de datos de estados del PIM.

Sintaxis:

summary pim

Ejemplo:

```
PIM>s
                Summary PIM State Database
                -----
0)  Group: 224.0.1.42
0)  Source: 9.37.179.1
0)  States: 1-P 2-P
```

PIM>

Group La dirección del grupo de destino asociada a la entrada.

Source La dirección de origen del originador del datagrama de difusión múltiple.

States Muestra las interfaces y los estados asociados al par de grupos de origen. P identifica un estado de poda.

Ping

Use el mandato **ping** para ejecutar ping dinámicamente a otra dirección de IPv6 de destino.

Sintaxis:

ping

Si desea ver un ejemplo de la salida de este mandato, vea la descripción del mandato **ping** en la sección IP Monitoring Commands del manual *Consulta de configuración y supervisión de protocolos Volumen 1*.

Consulte “Ping6” en la página 502 para obtener una descripción de los parámetros.

Reset

Use el mandato **reset** para restablecer PIM y volver a cargar la configuración.

Sintaxis:

reset

Ejemplo:

PIM>reset

Traceroute

Use el mandato **traceroute** para rastrear dinámicamente una ruta.

Sintaxis:

traceroute

Si desea ver un ejemplo de la salida de este mandato, vea la descripción del mandato **traceroute** en la sección IP Monitoring Commands del manual *Consulta de configuración y supervisión de protocolos Volumen 1*. Consulte “Traceroute6” en la página 503 si desea ver una descripción de los parámetros.

Variables

Use el mandato **variables** para visualizar información sobre las variables de configuración de PIM.

Sintaxis:

variables

Ejemplo:

PIM>variables

PIM: on

Graft Timeout: 3 seconds
Assert Timeout: 210 seconds

PIM Unicast Metric Preferences

Direct 0
Static 1
OSPF 110
RIP 120
BGP 200

PIM>

PIM: on/off

Indica si PIM-DM está actualmente habilitado o inhabilitado.

Graft Timeout

Número de segundos durante los cuales se vuelven a transmitir injertos si no se ha recibido acuse de recibo de injerto.

Assert Timeout

Número de segundos durante el cual la información de validación, obtenida por direccionadores de comunicaciones en sentido inverso, se retiene antes de volver a la información de direccionamiento local.

PIM Unicast Metric Preferences

Muestra las preferencias métricas del tipo de direccionamiento configurado actualmente. Cada tipo de ruta con soporte está en una lista con un valor decimal que muestra la preferencia métrica configurada actualmente.

Soporte de reconfiguración dinámica de PIM

Esta sección describe la reconfiguración dinámica (DR) en la medida en que afecta a los mandatos de Talk 6 y Talk 5.

Delete Interface de CONFIG (Talk 6)(Suprimir interfaz)

Protocol Independent Multicast (PIM) da soporte al mandato de CONFIG (Talk 6) **delete interface** sin ninguna restricción.

Activate Interface de GWCON (Talk 5)(Activar interfaz)

PIM da soporte al mandato de GWCON (Talk 5) **activate interface**, teniendo en cuenta lo siguiente:

PIM debe estar habilitado globalmente para poder activarlo en una interfaz de red.

Todos los mandatos específicos de la interfaz de PIM están soportados por el mandato de GWCON (Talk 5) **activate interface**.

Reset Interface de GWCON (Talk 5)(Restablecer interfaz)

PIM da soporte al mandato de GWCON (Talk 5) **reset interface**, teniendo en cuenta lo siguiente:

PIM debe estar habilitado globalmente para poder activarlo en una interfaz de red.

Todos los mandatos específicos de la interfaz de PIM están soportados por el mandato de GWCON (Talk 5) **reset interface**.

Mandatos Component Reset de GWCON (Talk 5)(Restablecer componente)

PIM da soporte a los siguientes mandatos **reset** de GWCON (Talk 5) específicos de PIM:

GWCON, Protocol PIM, Reset Command

Descripción: Restablece normalmente interfaces y valores de variable de PIM.

Efecto en la red: Pérdida de adyacencia de vecino de PIM en todas las interfaces que ejecutan PIM. Esto puede tener cierto impacto en el reenvío de difusión múltiple de IP, aunque se corrige la información después de un período de tiempo durante el que la adyacencia de vecino se establece de nuevo.

Limitaciones: Ninguna.

Todos los mandatos PIM están soportados por el mandato **GWCON, protocol pim, reset**.

Soporte de reconfiguración dinámica de PIM para IPv6

Esta sección describe la reconfiguración dinámica (DR) en la medida en que afecta a los mandatos de Talk 6 y Talk 5.

Delete Interface de CONFIG (Talk 6)(Suprimir interfaz)

Protocol Independent Multicast para IPv6 (PIM6) da soporte al mandato de CONFIG (Talk 6) **delete interface** sin ninguna restricción.

Activate Interface de GWCON (Talk 5)(Activar interfaz)

PIM6 da soporte al mandato de GWCON (Talk 5) **activate interface**, teniendo en cuenta lo siguiente:

PIM6 debe estar habilitado globalmente para poder activarlo en una interfaz de red.

Todos los mandatos específicos de la interfaz de PIM6 están soportados por el mandato de GWCON (Talk 5) **activate interface**.

Reset Interface de GWCON (Talk 5)(Restablecer interfaz)

PIM6 da soporte al mandato de GWCON (Talk 5) **reset interface**, teniendo en cuenta lo siguiente:

PIM6 debe estar habilitado globalmente para poder activarlo en una interfaz de red.

Todos los mandatos específicos de la interfaz de PIM6 están soportados por el mandato de GWCON (Talk 5) **reset interface**.

Mandatos Component Reset de GWCON (Talk 5)(Restablecer componente)

PIM6 da soporte a los siguientes mandatos de GWCON (Talk 5) **reset** específicos de PIM6:

GWCON, Protocol PIM, Reset Command

Descripción: Restablece dinámicamente interfaces y valores de variable de PIM6.

Efecto en la red: Pérdida de adyacencia de vecino de PIM6 en todas las interfaces que ejecutan PIM6. Esto puede tener cierto impacto en el reenvío de difusión múltiple de IPv6, aunque se corrige la información después de un período de tiempo durante el que la adyacencia de vecino se establece de nuevo.

Limitaciones: Ninguna.

Todos los mandatos PIM6 están soportados por el mandato **GWCON, protocol pim, reset**.

Soporte de reconfiguración dinámica de Multicast Forwarding Cache

Nota: Los mandatos siguientes son comunes entre MOSPF, DVMRP y PIM y son considerados mandatos MFC para IPv4:

- **join**
- **leave**
- **mcache**
- **mgroups**
- **mstats**

Consulte “Configuring and Monitoring OSPF” si desea tener más información sobre MOSPF y “Configuring and Monitoring DVMRP” si desea ver más información sobre DVMRP. Ambos capítulos se encuentran en *Consulta de configuración y supervisión de protocolos Volumen 1*.

Esta sección describe la reconfiguración dinámica (DR) en la medida en que afecta a los mandatos de Talk 6 y Talk 5.

Delete Interface de CONFIG (Talk 6)(Suprimir interfaz)

MulticastLa Multicast Forwarding Cache (MFC) da soporte al mandato **delete interface** de CONFIG (Talk 6), teniendo en cuenta lo siguiente:

IP debe notificar a MFC la actualización de direcciones.

Activate Interface de GWCON (Talk 5)(Activar interfaz)

MFC da soporte al mandato de GWCON (Talk 5) **activate interface**, teniendo en cuenta lo siguiente:

IP debe notificar a MFC la actualización de direcciones.

Todos los mandatos específicos de la interfaz de MFC están soportados por el mandato de GWCON (Talk 5) **activate interface**.

Reset Interface de GWCON (Talk 5)(Restablecer interfaz)

MFC da soporte al mandato de GWCON (Talk 5) **reset interface**, teniendo en cuenta lo siguiente:

IP debe notificar a MFC la actualización de direcciones.

Todos los mandatos específicos de la interfaz de MFC están soportados por el mandato de GWCON (Talk 5) **reset interface**.

Mandatos no reconfigurables dinámicamente

Todos los parámetros de configuración de MFC pueden cambiarse dinámicamente.

Soporte de reconfiguración dinámica de Multicast Forwarding Cache V6

Nota: Los siguiente mandatos de PIM se consideran mandatos de Multicast Forwarding Cache (MFC6) para IPv6:

- **join**
- **leave**
- **mcache**
- **mgroups**
- **mstats**

Esta sección describe la reconfiguración dinámica (DR) en la medida en que afecta a los mandatos de Talk 6 y Talk 5.

Delete Interface de CONFIG (Talk 6)(Suprimir interfaz)

MulticastLa Multicast Forwarding Cache V6 (MFC6) da soporte al mandato **delete interface** de CONFIG (Talk 6), teniendo en cuenta lo siguiente:

IPv6 debe notificar a MFC6 la actualización de direcciones.

Activate Interface de GWCON (Talk 5)(Activar interfaz)

MulticastLa Multicast Forwarding Cache V6 (MFC6) da soporte al mandato de GWCON (Talk 5) **activate interface**, teniendo en cuenta lo siguiente:

IPv6 debe notificar a MFC6 la actualización de direcciones.

Todos los mandatos de Multicast Forwarding Cache V6 (MFC6) específicos de la interfaz están soportados por el mandato de GWCON (Talk 5) **activate interface**.

Reset Interface de GWCON (Talk 5)(Restablecer interfaz)

MulticastLa Multicast Forwarding Cache V6 (MFC6) da soporte al mandato de GWCON (Talk 5) **reset interface** con las consideraciones siguientes:

IPv6 debe notificar a MFC6 la actualización de direcciones.

Todos los mandatos de Multicast Forwarding Cache V6 V6 (MFC6) específicos de la interfaz están soportados por el mandato de GWCON (Talk 5) **reset interface**.

Mandatos no reconfigurables dinámicamente

Todos los parámetros de configuración de Multicast Forwarding Cache V6 (MFC6) pueden cambiarse dinámicamente.

Configuración y supervisión de Routing Information Protocol (RIP6)

RIP6 es un protocolo de direccionamiento del vector de distancia. La configuración de RIP6 se efectúa en cada interfaz. Este capítulo describe cómo usar los mandatos de funcionamiento y de configuración de RIP6 e incluye las secciones siguientes:

- “Acceso al entorno de configuración de RIP6”
- “Mandatos de configuración de RIP6”
- “Acceso al entorno de supervisión de RIP6” en la página 547
- “Mandatos de supervisión de RIP6” en la página 547
- “Soporte de reconfiguración dinámica de RIP6” en la página 549

Acceso al entorno de configuración de RIP6

Siga el procedimiento siguiente para acceder al proceso de configuración de RIP6.

1. En el indicador OPCON, entre **talk 6**. (Para obtener información más detallada sobre este mandato, consulte “The OPCON Process and Commands” (Los mandatos y el proceso de OPCON) en *Guía del usuario de software*.) Por ejemplo:

```
* talk 6
Config>
```

Después de entrar el mandato **talk 6**, el indicador CONFIG (Config>) aparecerá en el terminal. Si el indicador no aparece cuando entre por primera vez en la configuración, pulse de nuevo **Retorno**.

2. En el indicador CONFIG, entre el mandato **p rip6** para obtener el indicador RIP66 Config>.

Mandatos de configuración de RIP6

Para configurar RIP6, entre los mandatos en el indicador RIP66 Config>.

Tabla 120 (Página 1 de 2). Resumen de los mandatos de configuración de RIP6

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte la sección “Cómo obtener ayuda” en la página xxix.
add	Añade RIP6 en una interfaz.
change	Cambia los valores de configuración métrica de RIP6 o el valor por omisión originario.
delete	Elimina RIP6 de una interfaz.
disable	Inhabilita RIP6 en una interfaz.
enable	Habilita RIP6 en una interfaz.
list	Lista la configuración.
set	Establece los valores métricos de RIP6.

Mandatos de configuración de RIP6 (Talk 6)

Tabla 120 (Página 2 de 2). Resumen de los mandatos de configuración de RIP6	
Mandato	Función
Exit	Le devuelve al nivel de mandatos anterior. Consulte la sección "Cómo salir de un entorno de nivel inferior" en la página xxix.

Add

Use el mandato **add** para añadir RIP6 a una interfaz.

Sintaxis:

add *núm.interfaz*

núm.interfaz

Especifica la interfaz a la que se añadirá el protocolo RIP6.

Nota: Esta interfaz debe tener configurada una dirección de IPv6 o ser la interfaz virtual de un túnel de IPv6 sobre IPV4.

Valores válidos: Cualquier número de interfaz válido

Valor por omisión: Ninguno

Change

Use el mandato **change** para cambiar un valor métrico de RIP6.

Sintaxis:

change *originating-default*
rip6-in-metric
rip6-out-metric

originating-default

Estos parámetros de configuración que se encuentran a continuación permiten cambiar el direccionador por omisión originario.

Always originate default route La habilitación de este parámetro permite a RIP6 anunciar el direccionador como direccionador por omisión (llamado "originario de la ruta por omisión"). El direccionador por omisión realiza el direccionamiento para otros direccionadores de Internet que tienen paquetes para un destino de red desconocido.

Valores válidos: Yes o No

Valor por omisión: No

Originate default dependent on BGP route availability Este campo permite al usuario habilitar o inhabilitar un direccionador que ejecuta EGP/BGP para anunciarse a sí mismo como direccionador por omisión por medio de su IGP (RIP6 en este caso.)

Valores válidos: Yes o No

Valor por omisión: No

From AS number Si está configurando RIP6 para que origine una ruta por omisión cuando haya rutas EGP disponibles, también puede configurarlo para que origine la ruta por omisión sólo si se reciben rutas EGP procedentes de un AS específico. Por ejemplo, si desea que se genere una ruta por omisión sólo si se recibe una ruta EGP procedente del AS número 12, debe establecer este parámetro en 12. Si establece el número de AS en 0, significa “procedente de cualquier AS.”

Valores válidos: 0 - 65535

Valor por omisión: Ninguno

Destination prefix (or network number) Si está originando una ruta por omisión cuando hay rutas EGP disponibles, también puede optar por originar la ruta por omisión sólo si se recibe una ruta específica a través del EGP. Por ejemplo, si desea que se genere una ruta por omisión sólo si se recibe una ruta a la red N, será necesario establecer este parámetro en N. Si establece el número de red en :: (cero) significa “cualquier ruta que se reciba.”

Valores válidos: Cualquier dirección de difusión individual IPv6, ninguna dirección de difusión múltiple, ninguna dirección de bucle de retorno, ninguna dirección de enlace local, ninguna dirección local de ubicación, ninguna dirección correlacionada por IPv4

Valor por omisión: Ninguno

Prefix length Longitud del prefijo. Este parámetro debe configurarse si **originate default if BGP routes available** es yes.

Valores válidos: 8 - 128

Valor por omisión:

Originate default if OSPF6 routes available Se puede configurar un direccionador que ejecute OSPF6 para que se anuncie a sí mismo como direccionador por omisión (llamado originario de la ruta por omisión) por medio de RIP6. Cuando este parámetro esté habilitado, el direccionador se anuncia a sí mismo como direccionador por omisión por medio de RIP6 si tiene rutas derivadas de OSPF6 en la tabla de direccionamiento. El direccionador por omisión realiza el direccionamiento para otros direccionadores de Internet que tienen paquetes para un destino de red desconocido.

Valores válidos: Yes o No

Valor por omisión: No

Originated default cost Este parámetro especifica el coste que RIP anunciará con la ruta por omisión que origina. El coste se utiliza para determinar la vía de acceso más corta para la ruta por omisión hacia el direccionador vecino de la misma.

Valores válidos: 1 - 16

Valor por omisión: 1

Ejemplo:

Mandatos de configuración de RIP6 (Talk 6)

```
RIP6 config>set originating
Always originate default route? [No]: Yes
Enter Originated default cost: between 1 and 15 [1]? 1
Update RIP6 default origination dynamically: OK
RIP6 config>
```

Ejemplo:

```
RIP6 config>set originating
Always originate default route? [Yes]: no
Originate default dependent on BGP6 route availability? [No]: yes
From AS number [0]? 10
Dest. prefix (or network number) [::]? 1234::0
Prefix length must between 8 and 128 [64]? 64
Enter Originated default cost: between 1 and 15 [1]? 1
Update RIP6 default origination dynamically: OK
RIP6 config>
```

rip6-in-metric

Cambia el valor de la métrica de RIP6 por las actualizaciones de llegada de RIP6.

Change RIPng metric on which interface? Especifica el número de la interfaz donde se va a cambiar la métrica de entrada de RIP6.

Nota: La interfaz debe tener configurado RIP6.

Valores válidos: Cualquier número de interfaz válido

Valor por omisión: 0

RIP6 input Metric Cambia el valor de la métrica de RIP6 en las actualizaciones de RIP6 de entrada.

Valores válidos: De 1 a 15

Valor por omisión: 1

rip6-out-metric

Cambia la métrica de RIP6 en las actualizaciones de RIP6 de salida.

Change RIPng metric on which interface? Especifica el número de la interfaz donde se va a cambiar la métrica de salida de RIP6.

Nota: La interfaz debe tener configurado RIP6.

Valores válidos: Cualquier número de interfaz válido

Valor por omisión: 0

RIP6 output Metric Especifica el valor de la métrica de RIP6 en las actualizaciones de RIP6 de salida.

Valores válidos: De 0 a 15

Valor por omisión: 0

Delete

Use el mandato **delete** para sacar RIP6 de la interfaz especificada.

Sintaxis:

delete *núm.interfaz*

núm.interfaz

Especifica la interfaz de la que se sacará el protocolo RIP6.

Nota: La interfaz debe tener configurado RIP6.

Valores válidos: Cualquier número de interfaz válido

Valor por omisión: Ninguno

Disable

Use el mandato **disable** para inhabilitar RIP6.

Sintaxis:

```
disable          override ...
                  rip6
                  sending ...
```

override ...

static-routes Altera temporalmente las rutas estáticas de RIP6 en una interfaz.

Modify RIP6 flags on which interface? Especifica el número de la interfaz donde se va a inhabilitar RIP6.

Nota: La interfaz debe tener configurado RIP6.

Valores válidos: Cualquier número de interfaz válido

Valor por omisión: 0

default Altera temporalmente las rutas por omisión de RIP6 en una interfaz.

Modify RIP6 flags on which interface? Especifica el número de la interfaz donde se va a inhabilitar RIP6.

Nota: La interfaz debe tener configurado RIP6.

Valores válidos: Cualquier número de interfaz válido

Valor por omisión: 0

rip6 Inhabilita RIP6 en la interfaz especificada.

Valores válidos: Yes o No

Valor por omisión: Yes

Modify RIP6 flags on which interface? Especifica el número de la interfaz donde se va a inhabilitar RIP6.

Nota: La interfaz debe tener configurado RIP6.

Valores válidos: Cualquier número de interfaz válido

Valor por omisión: 0

Mandatos de configuración de RIP6 (Talk 6)

sending ...

Modify RIP6 flags on which interface?

Especifica el número de la interfaz donde se va a inhabilitar RIP6.

Nota: La interfaz debe tener configurado RIP6.

Valores válidos: Cualquier número de interfaz válido

Valor por omisión: 0

all-routes

Inhabilita el anuncio de todas las rutas de RIP6 en una interfaz.

Valores válidos: Yes o No

Valor por omisión: Yes

default-routes

Inhabilita el anuncio de las rutas por omisión de RIP6 en una interfaz.

Valores válidos: Yes o No

Valor por omisión: Yes

static-routes

Inhabilita el anuncio de las rutas estáticas de RIP6 en una interfaz.

Valores válidos: Yes o No

Valor por omisión: Yes

poisoned-reverse-routes

Inhabilita la inversión de veneno al enviar actualizaciones de RIP6 a una interfaz.

Valores válidos: Yes o No

Valor por omisión: Yes

Enable

Use el mandato **enable** para habilitar RIP6.

Sintaxis:

```
enable           override ...  
                rip6  
                sending ...
```

override ...

static-routes Altera temporalmente las rutas estáticas de RIP6 en una interfaz.

Modify RIP6 flags on which interface? Especifica el número de la interfaz donde se va a habilitar RIP6.

Nota: La interfaz debe tener configurado RIP6.

Valores válidos: Cualquier número de interfaz válido

Valor por omisión: 0

default Altera temporalmente las rutas por omisión de RIP6 en una interfaz.

Modify RIP6 flags on which interface? Especifica el número de la interfaz donde se va a habilitar RIP6.

Nota: La interfaz debe tener configurado RIP6.

Valores válidos: Cualquier número de interfaz válido

Valor por omisión: 0

rip6 Habilita RIP6 en la interfaz especificada.

Valores válidos: Yes o No

Valor por omisión: Yes

Modify RIP6 flags on which interface? Especifica el número de la interfaz donde se va a habilitar RIP6.

Nota: La interfaz debe tener configurado RIP6.

Valores válidos: Cualquier número de interfaz válido

Valor por omisión: 0

sending ...

Modify RIP6 flags on which interface?

Especifica el número de la interfaz donde se va a habilitar RIP6.

Nota: La interfaz debe tener configurado RIP6.

Valores válidos: Cualquier número de interfaz válido

Valor por omisión: 0

all-routes

Habilita el anuncio de todas las rutas de RIP6 en una interfaz.

Valores válidos: Yes o No

Valor por omisión: Yes

default-routes

Habilita el anuncio de las rutas por omisión de RIP6 en una interfaz.

Valores válidos: Yes o No

Valor por omisión: Yes

static-routes

Habilita el anuncio de las rutas estáticas de RIP6 en una interfaz.

Valores válidos: Yes o No

Mandatos de configuración de RIP6 (Talk 6)

Valor por omisión: Yes

poisoned-reverse-routes

Habilita la inversión de veneno al enviar actualizaciones de RIP6 a una interfaz.

Valores válidos: Yes o No

Valor por omisión: Yes

List

Use el mandato **list** para visualizar la configuración de RIP6.

Sintaxis:

```
list all
```

Ejemplo:

```
RIP6>list all
RIP6
  Nets: - 0      RIP6: ENABLED
           Send: static routes
                Poison reverse enabled.
           Receive: Not override default and static routes
           RIP interface input metric: 1
           RIP interface output metric: 0

RIP6 default origination: BGP6(AS=10, net/prefix_len=1234::/64), cost = 1

Import BGP6 routes: enabled - AUTOTAG: enabled
```

Set

Use el mandato **set** para establecer los parámetros de configuración de RIP6.

Sintaxis:

```
set import bgp6 routes
      originating default
      rip6-in-metric
      rip6-out-metric
```

import bgp6 routes

Este parámetro especifica que las rutas que BGP6 ha conocido se importarán a la red de direccionamiento de RIP6. Sólo se importarán las rutas que aparezcan en las tablas de intercambio de entrada de BGP6. Todas las rutas se importan con un coste igual al coste de su tabla de direccionamiento.

Valores válidos: Yes o No

Valor por omisión: Yes

Si las rutas que BGP6 ha conocido son importadas en la red de direccionamiento de RIP6, puede configurarse el parámetro siguiente:

Enable autotag Este parámetro permite que RIP6 genere automáticamente códigos para las rutas BGP6. El valor de código es el número de AS del que se conoce la ruta.

Valores válidos: Yes o No

Valor por omisión: Yes

Ejemplo:

```
RIP6 config>set import
Import BGP6 routes?? [Yes]:
Enable AUTOTAG? [Yes]:
AUTOTAG is updated dynamically
```

originating default

Estos parámetros de configuración que se encuentran a continuación permiten establecer RIP6 para que anuncie el direccionador como direccionador por omisión.

Always originate default route La habilitación de este parámetro permite a RIP6 anunciar el direccionador como direccionador por omisión (llamado originario de la ruta por omisión). El direccionador por omisión realiza el direccionamiento para otros direccionadores de Internet que tienen paquetes para un destino de red desconocido.

Valores válidos: Yes o No

Valor por omisión: No

Originate default dependent on BGP route availability Este campo permite al usuario habilitar o inhabilitar un direccionador que ejecuta EGP/BGP para anunciarse a sí mismo como direccionador por omisión por medio de su IGP (RIP6 en este caso.)

Valores válidos: Yes o No

Valor por omisión: No

From AS number Si está configurando RIP6 para que origine una ruta por omisión cuando haya rutas EGP disponibles, también puede configurarlo para que origine la ruta por omisión sólo si se reciben rutas EGP procedentes de un AS específico. Por ejemplo, si desea que se genere una ruta por omisión sólo si se recibe una ruta EGP procedente del AS número 12, debe establecer este parámetro en 12. Si establece el número de AS en 0, significa "procedente de cualquier AS".

Valores válidos: 0 - 65535

Valor por omisión: Ninguno

Destination prefix (or network number) Si está originando una ruta por omisión cuando hay rutas EGP disponibles, también puede optar por originar la ruta por omisión sólo si se recibe una ruta específica a través del EGP. Por ejemplo, si desea que se genere una ruta por omisión sólo si se recibe una ruta a la red N, será necesario establecer este parámetro en N. Si establece el número de red en :: (cero) significa "cualquier ruta que se reciba".

Valores válidos: Cualquier dirección de difusión individual IPv6, ninguna dirección de difusión múltiple, ninguna dirección de bucle de retorno, ninguna dirección de enlace local, ninguna dirección local de ubicación, ninguna dirección correlacionada por IPv4

Mandatos de configuración de RIP6 (Talk 6)

Valor por omisión: Ninguno

Prefix length Longitud del prefijo. Este parámetro debe configurarse si **originate default if BGP routes available** es **yes**.

Valores válidos: 8 - 128

Valor por omisión:

Originate default if OSPF6 routes available Se puede configurar un direccionador que ejecute OSPF6 para que se anuncie a sí mismo como direccionador por omisión (llamado originario de la ruta por omisión) por medio de RIP6. Cuando este parámetro esté habilitado, el direccionador se anuncia a sí mismo como direccionador por omisión por medio de RIP6 si tiene rutas derivadas de OSPF6 en la tabla de direccionamiento. El direccionador por omisión realiza el direccionamiento para otros direccionadores de Internet que tienen paquetes para un destino de red desconocido.

Valores válidos: Yes o No

Valor por omisión: No

Originated default cost Este parámetro especifica el coste que RIP anunciará con la ruta por omisión que origina. El coste se utiliza para determinar la vía de acceso más corta para la ruta por omisión hacia el direccionador vecino de la misma.

Valores válidos: 1 - 16

Valor por omisión: 1

Ejemplo:

```
RIP6 config>set originating
Always originate default route? [No]: Yes
Enter Originated default cost: between 1 and 15 [1]? 1
Update RIP6 default origination dynamically: OK
RIP6 config>
```

Ejemplo:

```
RIP6 config>set originating
Always originate default route? [Yes]: no
Originate default dependent on BGP6 route availability? [No]: yes
From AS number [0]? 10
Dest. prefix (or network number) [::]? 1234::0
Prefix length must between 8 and 128 [64]? 64
Enter Originated default cost: between 1 and 15 [1]? 1
Update RIP6 default origination dynamically: OK
RIP6 config>
```

rip6-in-metric

Establece la métrica de RIP6 en las actualizaciones de RIP6 de entrada.

Change RIPng metric on which interface? Especifica el número de la interfaz donde se va a establecer la métrica de entrada de RIP6.

Valores válidos: Cualquier número de interfaz válido

Valor por omisión: 0

RIP6 input Metric Especifica el valor de la métrica de RIP6 usada en las actualizaciones de RIP6 de entrada.

Valores válidos: De 1 a 15

Valor por omisión: 1

rip6-out-metric

Establece la métrica de RIP6 usada en las actualizaciones de RIP6 de salida.

Change RIPng metric on which interface? Especifica el número de la interfaz en que se establecerá la métrica de salida de RIP6.

Valores válidos: Cualquier número de interfaz válido

Valor por omisión: 0

RIP6 output Metric Especifica el valor de la métrica usada en actualizaciones RIP6 de salida.

Valores válidos: De 0 a 15

Valor por omisión: 0

Acceso al entorno de supervisión de RIP6

Siga el procedimiento siguiente para acceder a los mandatos de supervisión de RIP6. Este proceso le dará acceso al proceso de supervisión de RIP6.

1. En el indicador OPCON, entre **talk 5**. (Para obtener información más detallada sobre este mandato, consulte "The OPCON Process" (El proceso OPCON) en el manual *Guía del usuario de software*.) Por ejemplo:

```
* talk 5
+
```

Después de entrar el mandato **talk 5**, el indicador de GWCON (+) aparecerá en el terminal. Si el indicador no aparece cuando entre por primera vez en la configuración, pulse de nuevo **Retorno**.

2. En el indicador +, entre el mandato **p rip6** para ir al indicador RIP6>.

Ejemplo:

```
+ p rip6
RIP6>
```

Mandatos de supervisión de RIP6

Esta sección describe los mandatos de supervisión de RIP6.

Tabla 121 (Página 1 de 2). Resumen de los mandatos de supervisión de RIP6

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte la sección "Cómo obtener ayuda" en la página xxix.
dump	Muestra las tablas de direccionamiento.
list	Muestra la configuración.
ping6	Ejecuta ping dinámicos en una dirección de IPv6.

Mandatos de supervisión de RIP6 (Talk 5)

Tabla 121 (Página 2 de 2). Resumen de los mandatos de supervisión de RIP6

Mandato	Función
reset	Restablece dinámicamente RIP6.
traceroute6	Rastrea dinámicamente una ruta.
Exit	Le devuelve al nivel de mandatos anterior. Consulte la sección “Cómo salir de un entorno de nivel inferior” en la página xxix.

Dump

Consulte “Dump routing tables” en la página 524 para obtener información sobre el mandato **dump**.

List

Use el mandato **list** para visualizar la configuración.

Sintaxis:

list

Ejemplo:

```
RIP6>list
```

```
RIP6
Intf   State           In   Out
Metric Metric Send-Flags   Receive-Flags
0      Enabled /UP    1    0    St,P
```

```
Send Flags: St=Static D=Default P=PoisonReverse
Recv Flags: OSt=Override-Static OD=Override-Default
```

```
RIP originates default with cost 1 under these conditions:
  BGP6 or OSPF6 External route 1234::/64 from AS 10 available
  Default origination conditions not satisfied
Import BGP6 routes: enabled - AUTOTAG: enabled
```

Ping6

Consulte “Ping6” en la página 502 para obtener detalles sobre el mandato **ping6**.

Reset

Sintaxis:

reset

Ejemplo:

```
RIP6>reset
```

Traceroute6

Consulte “Traceroute6” en la página 503 para obtener información detallada sobre el mandato **traceroute6**.

Soporte de reconfiguración dinámica de RIP6

Esta sección describe la reconfiguración dinámica (DR) en la medida en que afecta a los mandatos de Talk 6 y Talk 5.

Delete Interface de CONFIG (Talk 6)(Suprimir interfaz)

Routing Information Protocol para IPv6 (RIP6) da soporte al mandato de CONFIG (Talk 6) **delete interface**, teniendo en cuenta lo siguiente:

Todas las configuraciones de RIP6 que se han configurado para esta interfaz también se suprimen.

Activate Interface de GWCON (Talk 5)(Activar interfaz)

RIP6 da soporte al mandato de GWCON (Talk 5) **activate interface**, teniendo en cuenta lo siguiente:

IPv6 debe estar configurado para esta interfaz

Todos los mandatos específicos de la interfaz de RIP6 están soportados por el mandato de GWCON (Talk 5) **activate interface**.

Reset Interface de GWCON (Talk 5)(Restablecer interfaz)

RIP6 da soporte al mandato de GWCON (Talk 5) **reset interface**, teniendo en cuenta lo siguiente:

Todas las configuraciones de RIP6 para una interfaz cambian dinámicamente si hay una dirección IPv6 configurada para dicha interfaz.

Todos los mandatos específicos de la interfaz de RIP6 están soportados por el mandato de GWCON (Talk 5) **reset interface**.

Mandatos Component Reset de GWCON (Talk 5)(Restablecer componente)

Routing Information Protocol para IPv6 (RIP6) da soporte a los siguientes mandatos **reset** de GWCON (Talk 5) específicos de RIP6:

Mandato GWCON, Protocol RIP6 Reset Interface (o All Interfaces)

Descripción: Cambia dinámicamente las políticas o parámetros de una interfaz de RIP6 (todas las interfaces de RIP6.)

Efecto en la red: Dependiendo de los cambios de configuración, alterará las políticas de envío o recibo de las rutas RIP6 en una interfaz.

Limitaciones: Ninguna.

Todos los mandatos RIP6 están soportados por el mandato **GWCON, protocol RIP6 reset interface (o all interfaces)**.

Mandatos Immediate Change de CONFIG (Talk 6)(Cambio inmediato)

RIP6 da soporte a los siguientes mandatos de CONFIG que cambian inmediatamente el estado operativo del dispositivo. Estos cambios se guardan y se conservan si se vuelve a cargar o se reinicia el dispositivo, o si se ejecuta un mandato reconfigurable dinámicamente.

Todos los mandatos Talk 6 de RIP6 son dinámicos.

Mandatos no reconfigurables dinámicamente

Todos los parámetros de configuración de RIP6 pueden cambiarse dinámicamente.

Configuración y supervisión de BGP6

El protocolo BGP4 con la adición de RFC 2283, *Multiprotocol Extensions for BGP4 (BGP4+)*, da soporte a la información de direccionamiento de IPv6.

Este capítulo describe los mandatos de configuración y supervisión de BGP6 e incluye las secciones siguientes:

- “Mandatos de configuración de BGP6”
- “Acceso al entorno de configuración de BGP6”
- “Acceso al entorno de supervisión de BGP6” en la página 568
- “Mandatos de supervisión de BGP6” en la página 568
- “Soporte de reconfiguración dinámica de BGP6” en la página 577

Acceso al entorno de configuración de BGP6

Para acceder al entorno de configuración de BGP6, entre el mandato siguiente en el indicador Config>:

```
Config> protocol bgp6
BGP6 Config>
```

Mandatos de configuración de BGP6

Esta sección describe los mandatos de configuración de BGP6. Estos mandatos permiten modificar el comportamiento del protocolo BGP6 para que se ajuste a necesidades específicas. Es necesaria cierta cantidad de información para producir un direccionador BGP6 plenamente funcional. Entre los mandatos de configuración de BGP6 en el indicador BGP6 Config>.

Tabla 122 (Página 1 de 2). Resumen de los mandatos de configuración de BGP6

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte la sección “Cómo obtener ayuda” en la página xxix.
Add	Añadir políticas y vecinos BGP6.
Attach	Une una lista de política de envío y recepción a un vecino en particular.
Change	Modifica información que se ha entrado originalmente con el mandato add .
Delete	Suprime información de configuración BGP6 que se ha entrado previamente con el mandato add .
Disable	Inhabilita ciertas funciones de BGP6 que el mandato enable ha activado.
Enable	Habilita hablantes BGP6, vecinos BGP6.
List	Muestra elementos de configuración de BGP6.

Mandato	Función
Move	Cambia el orden en el que se definen las políticas y los agregados.
Set	Establece el IPv6-route-table-scan-timer.
Update	Manipula una política de un nombre de lista de política configurado utilizando los mandatos add , delete , change y move del submenú.
Exit	Le devuelve al nivel de mandatos anterior. Consulte la sección “Cómo salir de un entorno de nivel inferior” en la página xxix.

Add

Use el mandato **add** para añadir información de BGP6 a la configuración.

Sintaxis:

```
add          aggregate . . .  
              neighbor . . .  
              no-receive asnum . . .  
              originate-policy . . .  
              policy-list . . .  
              receive-policy . . .  
              send-policy . . .
```

aggregate *prefijo red Longitud prefijo*

El mandato **add aggregate** hace que el hablante BGP6 agregue un bloque de direcciones y anuncie una única ruta a sus vecinos BGP6. Es necesario especificar el prefijo de red común a todas las rutas que se agregan, así como también la longitud del prefijo. El ejemplo siguiente muestra cómo agregar un bloque de direcciones.

1. **Network prefix** (Prefijo de red) especifica las direcciones que se ven afectadas. El prefijo es la primera dirección de un rango de direcciones especificado en una política de BGP6.

Valores válidos: una dirección IPv6 de difusión individual válida o una dirección IPv4 compatible, excluyendo las siguientes:

- direcciones de enlace local (FE80::)
- direcciones de ubicación local (FEC0::)
- dirección de bucle de retorno (::1)
- direcciones IPv6 correlacionadas con IPv4 (::FFFF:<dirección IPv4>)

Valor por omisión: ninguno

2. **Prefix length** (Longitud de prefijo) es aplicable a la dirección que se especifica en el prefijo de red para generar una dirección utilizada en una política de BGP6.

Valores válidos: 8 - 128

Valor por omisión: 64

Ejemplo: add aggregate

```
Network Prefix []? 2000::
Prefix Length [64]? 16
```

Cuando añade una definición de agregación, recuerde definir una política para impedir que se exporten las rutas agregadas. Si no lo hace, el direccionador anunciará tanto las rutas individuales y la agregada que ha definido. Esto no es aplicable cuando está agregando las rutas, que se originan desde la tabla de direccionamiento IGP.

neighbor *dirección vecino núm.AS temp.inic. temp.conex. temp.espera.
temp.keep alive tamaño segmento tcp*

Use el mandato **add neighbor** para definir un vecino BGP6. El vecino puede ser interno al AS del hablante BGP6 o externo. Para activar este vecino dinámicamente, use el mandato **reset neighbor** de supervisión de BGP6.

Neighbor address La **dirección de vecino** es la dirección IPv6 del vecino con el que desea tener una relación de igual a igual. Puede estar dentro del propio sistema autónomo o en otro sistema autónomo. Si se trata de un vecino externo, ambos hablantes BGP6 deben compartir la misma red. Dicha restricción no es aplicable a los vecinos internos.

Valores válidos: una dirección IPv6 de difusión individual válida o una dirección IPv4 compatible, excluyendo las siguientes:

- direcciones de enlace local (FE80::)
- direcciones de ubicación local (FEC0::)
- dirección de bucle de retorno (::1)
- direcciones IPv6 correlacionadas con IPv4 (::FFFF:<dirección IPv4>)
- dirección cero (::0)

Valor por omisión: ninguno

AS# El **núm.AS** es el número de sistema autónomo propio para el número de sistema autónomo del vecino o vecino interno. El número de AS del vecino tiene:

Valores válidos: Un entero en el rango de 1 a 65535

Valor por omisión: 1

Init timer **Temp.inic.** especifica la cantidad de tiempo que el hablante BGP6 espera antes de inicializar recursos y reiniciar la conexión de transporte con el vecino en caso de que el hablante haya cambiado previamente al estado IDLE (DES-OCUPADO) debido a un error. Si el error persiste, este temporizador crece exponencialmente.

Valores válidos: de 0 a 65535 segundos.

Valor por omisión: 12 segundos

Connect timer **Temp.conex.** especifica la cantidad de tiempo que el hablante BGP6 espera antes de reiniciar la conexión de transporte con su vecino si la conexión TCP es anómala

Mandatos de configuración de BGP6 (Talk 6)

mientras está en estado CONNECT (CONECTADO) o ACTIVE (ACTIVO). Mientras tanto, el hablante BGP6 continúa atento para escuchar cualquier conexión que el vecino pueda iniciar.

Valores válidos: de 0 a 65535 segundos.

Valor por omisión: 120 segundos

Hold timer Entre el **temp.espera** para especificar la longitud de tiempo que el hablante BGP6 espera antes de asumir que el vecino es inalcanzable. Ambos vecinos intercambian la información configurada en el mensaje OPEN y eligen el más pequeño de los dos temporizadores como valor de temporizador de espera negociado.

Cuando los vecinos ya han establecido la conexión BGP6, intercambian mensajes Keepalive a intervalos frecuentes para asegurarse de que la conexión todavía permanece activa y de que los vecinos están alcanzables. El intervalo del temporizador Keep-Alive se calcula que sea un tercio del valor del temporizador de espera negociado. Por lo tanto el valor del temporizador de espera debe ser cero o por lo menos tres segundos.

Tenga en cuenta que, en líneas conmutadas, podría utilizar el valor cero para el temporizador de espera para ahorrar ancho de banda al no enviar mensajes Keepalive a intervalos frecuentes.

Valores válidos: de 0 a 65535 segundos.

Valor por omisión: 90 segundos

TCP segment size El **Tamaño segmento TCP** especifica el tamaño máximo de datos que se pueden intercambiar en la conexión TCP con un vecino. Este valor se utiliza para una conexión TCP activa con el vecino.

Valores válidos: de 1 a 65535 bytes.

Valor por omisión: 1220 bytes

Ejemplo: `add neighbor`

```
Neighbor address []? 2002:9::6205
AS [1]? 2002
Init timer [12]?
Connect timer [120]?
Hold timer [90]?
TCP segment size [1220]?
```

no-receive *núm.AS*

Use el mandato **add no-receive** **núm.AS** para excluir vías de acceso de AS si el número de AS específico aparece en algún lugar dentro de la lista de vías de acceso de AS.

El **núm.AS** tiene:

Valores válidos: de 1 a 65535

Valor por omisión: 1

Ejemplo: `add no-receive`

Enter AS: [1]? 2003

originate-policy (*exclusiva/ inclusiva*) *prefijo red Longitud prefijo coincid. direcc. (Exacta/Rango) código*

Use el mandato **add originate-policy** para especificar el valor a utilizar al seleccionar rutas para anunciar.

Exclusiva Las políticas exclusivas impiden que se incluya la información de ruta en la tabla de direccionamiento del hablante BGP6.

Inclusiva Las políticas inclusivas aseguran la inclusión de rutas específicas en la tabla de direccionamiento del hablante BGP6.

Network prefix El parámetro Prefijo de red especifica la dirección de red que se ve afectada por esta política.

Valores válidos: una dirección IPv6 de difusión individual válida o una dirección IPv4 compatible, excluyendo las siguientes:

- direcciones de enlace local (FE80::)
- direcciones de ubicación local (FEC0::)
- dirección de bucle de retorno (::1)
- direcciones IPv6 correlacionadas con IPv4 (::FFFF:<dirección IPv4>)

Valor por omisión: ninguno

Prefix length **Longitud de prefijo** es aplicable a la dirección que se especifica en el prefijo de red para generar una dirección utilizada en una política de BGP6.

Valores válidos: De 0 a 128

Valor por omisión: 0

Address match Dirección o rango de direcciones que se verán afectadas por la declaración de política.

Valores válidos: Exacto o rango

Valor por omisión: Rango

Código El valor de código representa el número de AS del que se conoce la ruta. El valor de código se utiliza para interactuar con un IGP, como RIP6. Consulte la sección "Set" en la página 544 si desea obtener información acerca de la importación de rutas BGP6 y la generación de autocódigos BGP6.

Valores válidos: De 0 a 65535

Valor por omisión: 0

El ejemplo siguiente incluye todas las rutas de la tabla de direccionamiento IGP del hablante BGP6 que deberán anunciarse.

Ejemplo: `add originate-policy inclusive`

Mandatos de configuración de BGP6 (Talk 6)

Network Prefix [::]?
Prefix length[0]?
Address Match (Exact/Range) [Range]?
Tag [0]?

policy-list

Use el mandato **add policy-list** para configurar un grupo de políticas, que puede conectar con un vecino específico utilizando el mandato **attach policy-to-neighbor**.

Name Especifica el nombre a utilizar para identificar el grupo de políticas.

Valores válidos: Una serie de 1 a 15 caracteres ASCII

Valor por omisión: Ninguno

Ejemplo: add policy-list

Name[]? **nbr1-rcv**
Policy Type(Receive/Send) [Receive]? **Receive**

Ejemplo: add policy-list

Name[]? **nbr1-snd**
Policy Type(Receive/Send) [Receive]? **Send**

receive-policy (*exclusiva/ inclusiva*) *prefijo red Longitud prefijo coinc. direcc. núm.AS orig. núm.AS adyac. métrica igp (sólo inclusiva)*

Use el mandato **add receive-policy** para determinar las rutas que se importarán a la tabla de direccionamiento del hablante BGP6.

Las políticas exclusivas impiden que se incluya la información de ruta en la tabla de direccionamiento del hablante BGP6.

Las políticas inclusivas aseguran la inclusión de rutas específicas en la tabla de direccionamiento del hablante BGP6.

Network prefix El Prefijo de red especifica las direcciones que se ven afectadas.

Valores válidos: una dirección IPv6 de difusión individual válida o una dirección IPv4 compatible, excluyendo las siguientes:

- direcciones de enlace local (FE80::)
- direcciones de ubicación local (FEC0::)
- dirección de bucle de retorno (::1)
- direcciones IPv6 correlacionadas con IPv4 (::FFFF:<dirección IPv4>)

Valor por omisión: ninguno

Prefix Length La **longitud de prefijo** es aplicable a la dirección especificada en **network prefix** para generar una dirección utilizada en una política BGP6.

Valores válidos: De 0 a 128

Valor por omisión: 0

Address match Coinc. direcc. es un rango de direcciones o una dirección exacta.

Valores válidos: Exacto o rango

Valor por omisión: Rango

Originating AS# Un **núm.AS orig.** tiene:

Valores válidos: de 0 a 65535

Valor por omisión: 0

Adjacent AS# El **núm.AS adyac.** especifica el número de AS vecino.

Valores válidos: de 0 a 65535

Valor por omisión: 0

IGP metric La **métrica IGP**(sólo para políticas de recepción inclusivas) especifica el valor de métrica con el que las rutas aceptadas se importan a la tabla de direccionamiento IGP del hablante. Si la métrica IGP es -1, estas rutas no se importarán en el IGP; por lo tanto, estas rutas no pueden volver a anunciarse.

Valores válidos: de -1 a 65535

Valor por omisión: 0

Ejemplo: **add receive-policy exclusive**

```
Network Prefix [::]? 2003::
Prefix length[0]? 16
Address Match (Exact/Range) [Range]?
Originating AS# [0]? 168
Adjacent AS# [0]? 165
```

Ejemplo: **add receive-policy inclusive**

```
Network Prefix [::]? 2000:: Prefix Length [0]? 64
Address Match (Exact/Range) [Range]?
Originating AS# [0]?
Adjacent AS# [0]?
IGP-metric [0]?
```

send-policy (*exclusiva/ inclusiva*) *prefijo red Longitud prefijo coinc. direcc. código núm.AS adyac.*

Use el mandato **add send-policy** para crear políticas que determinan cuál de las rutas conocidas por el hablante BGP6 se volverá a anunciar. Estas rutas pueden ser internas o externas al AS del hablante BGP6.

Las políticas exclusivas impiden que la información de ruta de la tabla de direccionamiento del hablante BGP6 sea anunciada a los vecinos BGP6.

Las políticas inclusivas aseguran que las rutas específicas de la tabla de direccionamiento del hablante BGP6 sean anunciadas a los vecinos BGP6.

Network prefix El **prefijo red** es para las direcciones que se ven afectadas.

Valores válidos: una dirección IPv6 de difusión individual válida o una dirección IPv4 compatible, excluyendo las siguientes:

- direcciones de enlace local (FE80::)
- direcciones de ubicación local (FEC0::)
- dirección de bucle de retorno (::1)
- direcciones IPv6 correlacionadas con IPv4 (::FFFF:<dirección IPv4>)

Valor por omisión: ninguno

Mandatos de configuración de BGP6 (Talk 6)

Prefix length Longitud de prefijo es aplicable a la dirección que se especifica en el prefijo de red para generar una dirección utilizada en una política de BGP6.

Valores válidos: De 0 a 128

Valor por omisión: 0

Address match Coinc. direcc. es un rango de direcciones o una dirección exacta.

Valores válidos: Exacto o rango

Valor por omisión: Rango

Código El valor de código representa el número de AS del que se conoce la ruta. El valor de código se utiliza para interactuar con un IGP, como RIP6. Consulte la sección "Set" en la página 544 si desea obtener información acerca de la importación de rutas BGP6 y la generación de autocódigos BGP6.

Valores válidos: de 0 a 65535

Valor por omisión: 0

Adjacent AS# El núm.AS adyac. especifica el número de AS vecino.

Valores válidos: de 0 a 65535

Valor por omisión: 0

Ejemplo: `add send exclusive`

```
Network Prefix []? 2003::  
Prefix length[0]? 16  
Address Match (Exact/Range) [Range]?  
Tag [0]?  
Adjacent AS# [0]?
```

Attach

Use el mandato **attach policy-to-neighbor** para conectar un nombre de lista de política configurado a un vecino específico. Se pueden conectar hasta tres nombres de lista de política de envío y tres de recepción.

Sintaxis:

```
attach                policy-to-neighbor
```

Ejemplo: attach policy-to-neighbor

```
Neighbor address [::]? 2003::  
First receive policy list name (none for global AS based policy)[]? nbr1-rcv  
Second receive policy list name (none for exit)[]?  
First send policy list name (none for global AS based policy)[]? nbr1-snd  
Second send policy list name (none for exit)[]?
```

Change

Use el mandato **change** para cambiar un elemento de configuración de BGP6 instalado anteriormente por el mandato add.

Sintaxis:

```
change                aggregate . . .  
                        neighbor . . .
```

```

originate-policy . . .
policy-to-neighbor
receive-policy . . .
send-policy. . .

```

aggregate *núm.índice prefijo red Long.prefijo*

Este ejemplo cambia el agregado actual (aggregate 1).

Ejemplo: **change aggregate 1**

```

Network Prefix [2000:~?] 2001::
Prefix Length [16]?

```

neighbor *dirección IPv6 vecino núm.AS temp.inic. temp.conex. temp.espera temp.keep alive tamaño segmento tcp*

Use este mandato para cambiar los valores de los parámetros de configuración de un vecino ya existente. Este mandato no puede utilizarse para cambiar la dirección de un vecino ya existente.

Para reactivar el vecino dinámicamente, use el mandato **reset neighbor** de supervisión BGP6.

La **dirección de vecino** a modificar tiene:

Valores válidos: Cualquier dirección de vecino configurada actualmente

Valor por omisión: ninguno

El ejemplo siguiente cambia el valor del temporizador de espera a cero para el vecino 2002:0::6205.

Ejemplo: **change neighbor 2002:0::6205**

```

AS [2002]?
Init timer [12]?
Connect timer [60]?
Hold timer [12]? 0
TCP segment size [1220]?

```

originate-policy *núm.índice (exclusiva/ inclusiva) prefijo red Longitud prefijo coincid. direcc. código*

Use el mandato **change originate-policy** para alterar una definición de política originaria ya existente.

Este ejemplo altera la política originaria del hablante BGP6.

Ejemplo: **change originate-policy**

```

Enter index of originate-policy to be modified [1]?
Policy Type (Inclusive/Exclusive) [Exclusive]? inclusive
Network Prefix [2003:~?] 2004::
Prefix Length [16]? 16
Address Match (Exact/Range) [Range]?
Tag [0]?

```

policy-to-neighbor

Use el mandato **change policy-to-neighbor** para cambiar una conexión de lista de política con un vecino en particular.

Ejemplo: **change policy-to-neighbor**

```

Neighbor address [0:~0]? 2003::
First receive policy list name to be changed[nbr1-rcv]?
Second receive policy list name to be changed[]?
Third receive policy list name to be changed[]?
First send policy list name to be changed[nbr1-snd]?
Second send policy list name to be changed[]?
Third send policy list name to be changed[]?

```

Mandatos de configuración de BGP6 (Talk 6)

receive-policy *núm.índice (exclusiva/inclusiva) prefijo red Longitud prefijo coinc. direcc. núm.AS orig. núm.AS adyac. métrica igp (sólo inclusiva)*
Use el mandato **change receive-policy** para alterar una definición de política de recepción ya existente.

Este ejemplo añade una restricción a la política de recepción del hablante BGP6. En lugar de importar información de ruta de cada igual BGP6 a la tabla de direccionamiento IGP, ahora impedirá la importación de las rutas a partir de AS 165.

Ejemplo: change receive-policy

```
Enter index of receive-policy to be modified [1]?
Policy Type (Inclusive/Exclusive) [Inclusive]? exclusive
Network Prefix [2003::]?
Prefix Length [16]?
Address Match (Exact/Range) [Range]?
Originating AS# [0]?
Adjacent AS# [0]? 165
```

send-policy *núm.índice (exclusiva/inclusiva) prefijo red Longitud prefijo coinc.direcc. código núm.AS adyac.*
Use el mandato **change send-policy** para alterar una política de envío ya existente por una que es más inclusiva o más exclusiva.

Este ejemplo añade una restricción a la política de envío del hablante BGP6.

Ejemplo: change send-policy

```
Enter index of send-policy to be modified [1]?
Policy Type (Inclusive/Exclusive) [Inclusive]? exclusive
Network Prefix [0::0]? 2004:6::6205
Prefix Length [16]? 16
Address Match (Exact/Range) [Range]?
Tag [0]?
Adjacent AS# [0]? 165
```

Delete

Use el mandato **delete** para suprimir un elemento de configuración de BGP6 instalado previamente por el mandato **add**.

Sintaxis:

delete aggregate . . .
neighbor . . .
no-receive . . .
originate-policy . . .
policy-list . . .
policy-to-neighbor
receive-policy . . .
send-policy. . .

aggregate *núm.índice*

Debe especificar el número de índice del agregado que desea suprimir.

Ejemplo: delete aggregate 1

neighbor *dirección IPv6 vecino*

Use este mandato para suprimir un vecino BGP6. Debe especificar la dirección de red del vecino.

La **dirección de red del vecino a suprimir** tiene:

Valores válidos: Cualquier dirección de vecino configurada actualmente

Valor por omisión: ninguno

Para desactivar este vecino dinámicamente use el mandato **reset neighbor** de supervisión de BGP6.

Ejemplo: delete neighbor 2002:9::6024

no-receive *núm.AS*

Use este mandato para suprimir la política de no recepción configurada para un AS en particular. Debe especificar el número de AS.

El **núm.AS** tiene:

Valores válidos: de 1 a 65535

Valor por omisión: ninguno

Ejemplo: delete no-receive 168

originate-policy *núm.índice*

Use este mandato para suprimir una política originaria específica. Debe especificar el número de índice asociado con la política.

Ejemplo: delete originate-policy 2

policy-list

Use el mandato **delete policy-list** para suprimir una lista de política.

Ejemplo: delete policy-list

```
Name of policy-list to delete []? nbr1-rcv
All policies defined for 'nbr1-rcv' will be deleted.
Are you sure you want to delete (Yes or [No])? Yes
Policy-list 'nbr1-rcv' is deleted.
```

La conexión de política a vecino se ajustará según sea necesario.

policy-to-neighbor

Use el mandato **delete policy-to-neighbor** para suprimir una conexión de nombre de lista de política ya existente a un vecino en particular.

Ejemplo: delete policy-to-neighbor

```
Neighbor address []? 2009:9::6205
Remove first receive policy-list name [nbr1-rcv]
Are you sure you want to remove (Yes or [No])? yes
Remove first send policy-list name [nbr1-snd]
Are you sure you want to remove (Yes or [No])? yes
```

receive-policy *núm.índice*

Use este mandato para suprimir una política de recepción específica. Debe especificar el número de índice asociado con la política.

Ejemplo: delete receive-policy

```
Enter index of receive-policy to be deleted [1]?
```

send-policy *núm.índice*

Use este mandato para suprimir una política de envío específica. Debe especificar el número de índice asociado con la política.

Ejemplo: delete send-policy 4

Disable

Use el mandato **disable** para inhabilitar un hablante o vecino BGP6 previamente habilitado. Tenga en cuenta que los vecinos se habilitan implícitamente siempre que se añaden con el mandato **add**.

Sintaxis:

```
disable          BGP6 speaker
                  compare-med-from-diff-AS
                  neighbor . . .
```

BGP6 speaker

Use el mandato **disable BGP6 speaker** para inhabilitar el protocolo BGP6.

Ejemplo: `disable BGP6 speaker`

compare-med-from-diff-AS

Use este mandato para inhabilitar una comparación MED entre distintos AS.

Ejemplo: `disable compare-med-from-diff-AS`

neighbor *dirección IPv6 vecino*

Use este mandato para inhabilitar un vecino actualmente configurado. La **dirección de vecino** tiene:

Valores válidos: Cualquier dirección IPv6 válida

Valor por omisión: ninguno

Ejemplo: `disable neighbor 2002:9::6205`

Enable

Use el mandato **enable** para activar la información, capacidades y características de BGP6 que se han añadido a la configuración BGP6.

Sintaxis:

```
enable          BGP6 speaker
                  compare-med-from-diff-AS
                  neighbor . . .
```

BGP6 speaker *núm.AS tamaño segmento tcp*

Use el mandato **enable BGP6 speaker** para habilitar el protocolo BGP6.

1. El **núm.AS** se asocia con este conjunto de direccionadores y nodos.

Valores válidos: de 1 a 65535

Valor por omisión: 1

2. Entre el **tamaño segmento TCP** (TCP segment size) para especificar el tamaño máximo de segmento que BGP6 debe utilizar para conexiones TCP pasivas.

Valores válidos: de 1 a 65535 bytes.

Valor por omisión: 1220 bytes

Ejemplo: `enable BGP6 speaker`

AS [0]? 165
TCP segment size [1220]?

compare-med-from-diff-AS

Use este mandato para habilitar la comparación MED entre distintos AS.

Ejemplo: `enable compare-med-from-diff-AS`

neighbor *dirección IPv6 vecino*

Use este mandato para habilitar un vecino BGP6.

La **dirección de vecino** tiene:

Valores válidos: Cualquier dirección de vecino configurada actualmente

Valor por omisión: ninguno

Ejemplo: `enable neighbor 2002:9::6205`

List

Use el mandato **list** para visualizar varias partes de datos de configuración BGP6, dependiendo del submandato específico que se ha invocado.

Sintaxis:

```
list          aggregate
              all
              BGP6 speaker
              neighbor
              no-receive
              originate-policy
              policy-list . . .
              policy-to-neighbor
              receive-policy
              send-policy
```

aggregate

Use el mandato **list aggregate** para todas las rutas agregadas definidas con el mandato **add aggregate**.

Ejemplo: `list aggregate`

```
Aggregation:
Index  Prefix/Prefix length
1      2000::/16
```

all

Use el mandato **list all** para listar los vecinos BGP6, políticas, rutas agregadas y registros 'no recibir como' en la configuración actual de BGP6.

Ejemplo: `list all`

Mandatos de configuración de BGP6 (Talk 6)

```
BGP6 Protocol:      Enabled
AS:                 710
TCP-Segment Size:  1220
```

Neighbors and their AS:

Address	State	AS	Init Timer	Conn Timer	Hold Timer	TCPSEG Size
2003:7:8:2::820	ENABLD	820	12	120	90	1220
2002:9::6205	ENABLD	2002	12	120	90	1220

Receive-Policies:

Index	Type	Prefix/Prefix length	Match Range	OrgAS	AdjAS	IGPmet
1	INCL	::/0	Range	0	0	0
2	EXCL	2003::/16	Range	0	0	

Send-Policies:

Index	Type	Prefix/Prefix length	Match Range	Tag	AdjAS
1	INCL	::/0	Range	0	0
2	EXCL	2003::/16	Range	0	0

Originate-Policies:

Index	Type	Prefix/Prefix Length	Match Range	Tag
1	INCL	::/0	Range	0
2	EXCL	2003::/16	Range	0

Aggregation:

Index	Prefix/Prefix Length
1	2000::/16

AS-PATH with following ASs will be discarded:
AS 2003
compare-med-from-diff-as is enabled.
IPv6-route-table-scan-timer value is 2 seconds.

BGP6 speaker

Use el mandato **list BGP6 speaker** para obtener información del hablante BGP6. La información se proporciona del modo siguiente:

Ejemplo: list BGP6 speaker

```
BGP6 Protocol:      Enabled
AS:                 165
TCP-Segment Size:  1220
```

neighbor Use el mandato **list neighbor** para obtener información de vecinos BGP6.

Ejemplo: list neighbor

Neighbors and their AS along with attached policy-list name(s):

Address	State	AS	Init Timer	Conn Timer	Hold Timer	TCPSEG Size
2003:7:8:2::820	ENABLD	820	12	120	90	1220
2002:9::6205	ENABLD	2002	12	120	90	1220

no-receive

Use el mandato **list no-receive** para obtener información de las definiciones no-receive-AS que se han añadido a la configuración BGP6.

Ejemplo: list no-receive

AS-PATH with following autonomous systems will be discarded:
AS 178
AS 165

originate-policy *todo índice prefijo*

Use el mandato **list originate-policy** para obtener información de las políticas originarias que se han añadido a la configuración BGP6.

Ejemplo: list originate-policy

```

Originate-Policies:
Index  Type  Prefix/Prefix Length      Match  Tag
1      INCL  ::/0                      Range  0
2      EXCL  2003::/16                 Range  0

```

policy-list

Use el mandato **list policy-list** para listar los nombres de lista de política configurados.

Ejemplo: list policy-list

```

BGP6 Config>li policy list
Policy list:
nbr1-rcv  Receive
nbr1-snd  Send

```

policy-to-neighbor

Use el mandato **list policy-to-neighbor** para listar las políticas conectadas con los vecinos.

Ejemplo: list policy-to-neighbor

```

Neighbor address      Receive      Send
2002:9::6205         rec1        send1

```

receive-policy adj-as-number todo o índice o prefijo

Use el mandato **list receive-policy** para obtener información acerca de las políticas de recepción que se han añadido a la configuración BGP6. Se pueden visualizar todas las políticas de recepción definidas para un AS o visualizar políticas por índice o número de prefijo.

Ejemplo: list receive-policy

```

Receive-Policies:
Index  Type  Prefix/Prefix length      Match  OrgAS  AdjAS  IGPmet
1      INCL  ::/0                      Range  0      0      0
2      EXCL  2003::/16                 Range  0      0

```

send-policy adj-as-number todo o índice o prefijo

Use el mandato **list send-policy** para visualizar información acerca de políticas de envío definidas para sistemas autónomos específicos. Se pueden visualizar todas las políticas de envío definidas para un AS, o también se pueden visualizar las políticas por índice o número de prefijo.

Ejemplo: list send-policy

```

Send-Policies:
Index  Type  Prefix/Prefix length      Match  Tag  AdjAS
1      INCL  ::/0                      Range  0    0
2      EXCL  2003::/16                 Range  0    0

```

Move

Use el mandato **move** para cambiar el orden en el que se han definido las políticas y los agregados. Esto cambia el orden en que el direccionador aplica las políticas existentes a la información de ruta. Antes de utilizar este mandato, es aconsejable utilizar el mandato **list** para ver las políticas que se han definido.

Sintaxis:

move **aggregate o originate-policy o receive-policy o send-policy**

Ejemplo:

Mandatos de configuración de BGP6 (Talk 6)

```
move originate-policy
Enter index of originate-policy to move [1]? 3
Move record AFTER record number [0]?
```

Set

Use el mandato **set** para establecer el IPv6-route-table-scan-timer. El valor IPv6-route-table-scan-timer se utiliza para establecer el intervalo de tiempo de exploración de la tabla de reenvío IPv6 para las actualizaciones de BGP6.

Sintaxis:

```
set                ipv6-route-table-scan-timer
                   Valores válidos: 1 to 10
                   Valor por omisión: 1
```

Ejemplo:

```
set ipv6-route-table-scan-timer
Timer Value in seconds [1]? 2
```

Update

Use el mandato y los submandatos **update** para manipular las políticas.

Sintaxis:

```
update            policy-list
```

Ejemplo de política de recepción:

```
update policy-list
Name[]? nbr1-rcv
```

Add

Use el mandato **Add** para añadir políticas de envío o recepción dentro del mandato **update**.

Ejemplo: Adición de una política de recepción

```

BGP6 Config>add POLICY-LIST
Policy-list name []? rec1
Policy Type (Receive/Send) [Receive]?
BGP6 Config>UPDATE POLICY-LIST
Policy-list name []? rec1
Policy-list rec1:Receive Config>add
Policy Type (Inclusive/Exclusive) [Exclusive]?
Network Prefix [::]? 1234::
Prefix Length [0]? 16
Address Match (Exact/Range) [Range]?
Originating AS# [0]?
Any AS# [0]?
Policy-list rec1:Receive Config>list
Receive Policy list for rec1:
Idx T Prefix/Length/Match          OrgAS AnyAS MED   Weight
LP   IGPm
1   E 1234::/16/R                    0     0

```

```

Policy-list rec1:Receive Config>add
Policy Type (Inclusive/Exclusive) [Exclusive]? inc
Network Prefix [::]? 5678::
Prefix Length [0]? 16
Address Match (Exact/Range) [Range]?
Originating AS# [0]?
Any AS# [0]?
MED [0]?
Local-pref [0]?
Weight [0]?
IGP-metric [0]?
Policy-list rec1:Receive Config>list
Receive Policy list for rec1:
Idx T Prefix/Length/Match          OrgAS AnyAS MED   Weight
LP   IGPm
1   E 1234::/16/R                    0     0
2   I 5678::/16/R                    0     0     0     0

```

Ejemplo: Adición de una política de recepción

```

BGP6 Config>add POLICY-LIST
Policy-list name []? send1
Policy Type (Receive/Send)
[Receive]? send
BGP6 Config>UPDATE POLICY-LIST
Policy-list name []? send1
Policy-list send1:Send Config>add
Policy Type (Inclusive/Exclusive) [Exclusive]? i
Network Prefix [::]? 1234::
Prefix Length [0]? 16
Address Match (Exact/Range) [Range]?
Originating AS# [0]?
Any AS# [0]?
Tag [0]?
MED [0]?
# of AS padding [0]?
Policy-list send1:Send Config>list
Send Policy list for send1:
Idx T Prefix/Length/Match          OrgAS AnyAS Tag   MED
ASpad
1   I 1234::/16/R                    0     0     0     0

```

Notas:

1. No habrá solicitud para los parámetros *MED*, *Pref.local*, *Peso* y *Métrica IGP* para la política de recepción exclusiva. Se utilizarán los valores *MED* y *Pref.local* del anuncio recibido si están configurados como valor '0'. El valor '0' del parámetro *Weight* indica que se ignore el valor de peso en el proceso de selección de ruta.

Mandatos de supervisión de BGP6 (Talk 5)

2. La solicitud de los valores de parámetro *MED* y *núm.relleno AS* tiene lugar sólo para las políticas de envío inclusivas.

Change

Use el mandato **change** para cambiar políticas dentro del comando **update**.

Ejemplo:

```
Enter index of receive-policy to be modified [1]?
```

Delete

Use el mandato **delete** para suprimir políticas dentro del mandato **update**.

Ejemplo:

```
Enter index of receive-policy to be deleted [1]?
```

Move

Use el mandato **move** para mover políticas dentro del mandato **update**.

Ejemplo:

```
Enter index of receive-policy to move [1]?  
Move record after record number [0]?
```

List

Use el mandato **list policy-list** para listar políticas de recepción dentro del mandato **update**.

Ejemplo: list policy-list

```
Receive Policy list for rec1:  
Idx T Prefix/Length/Match          OrgAS AnyAS MED  Weight  
LP   IGPm  
1   E 1234::/16/R                   0     0           0  
2   I 5678::/16/R                   0     0           0
```

Ejemplo de política de envío:

```
update policy-list  
Name[]? nbr1-rcv
```

Acceso al entorno de supervisión de BGP6

Para acceder al entorno de supervisión de BGP6, entre el mandato siguiente en el indicador +:

```
+ protocol bgp6  
BGP6>
```

Mandatos de supervisión de BGP6

Esta sección describe los mandatos de supervisión de BGP6. Estos mandatos permiten modificar el comportamiento del protocolo BGP6 para que se ajuste a necesidades específicas. Es necesaria cierta cantidad de información para producir un direccionador BGP6 plenamente funcional. Entre los mandatos de supervisión de BGP6 en el indicador de supervisión BGP6>.

Tabla 123. Resumen de los mandatos de supervisión de BGP6

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte la sección "Cómo obtener ayuda" en la página xxix.
Disable neighbor	Inhabilita un vecino específico o todos los vecinos.
Dump routing tables	Lista el contenido de la tabla de direccionamiento de IPv6.
List	Lista todas las entradas de la tabla de direccionamiento de BGP.
Enable neighbor	Habilita un vecino específico o todos los vecinos.
Neighbors	Muestra los vecinos actualmente activos.
Parameter	Muestra los valores globales de BGP6 instalados en el sistema BGP6.
Paths	Muestra todas las vías de acceso disponibles en la base de datos.
Ping6	Envía solicitudes de eco ICMP a otro sistema principal una vez cada segundo y espera una respuesta. Este mandato puede utilizarse para aislar problemas en un entorno entre redes.
Policy-list	Muestra la política instalada actualmente para estadísticas de uso y un vecino específico de cada política.
Reset neighbor	Restablece un vecino específico.
Traceroute6	Muestra la vía de acceso completa (salto a salto) hacia un destino específico.
Exit	Le devuelve al nivel de mandatos anterior. Consulte la sección "Cómo salir de un entorno de nivel inferior" en la página xxix.

Disable Neighbor

Use el mandato **disable neighbor** para inhabilitar un vecino específico o todos los que se han habilitado. Este mandato desactiva la sesión BGP6 y elimina las rutas conocidas a partir de dicho vecino.

Sintaxis:

disable neighbor *dirección IPv6 vecino*

Ejemplo: **disable neighbor**

```
Enter a Neighbor address or :: for all neighbors []? ::
neighbor 2003:1::6105 disabled
```

Dump Routing Tables

Si desea obtener una explicación completa del mandato **dump routing tables**, consulte el mandato **Dump Routing Tables** en la página “Vuelco de tablas de direccionamiento” en la página 498.

Ejemplo:

Type	Dest net/Prefix	Cost	Age	Next hop(s)/Net
BGPR	2001:6::/64	0	193	IP64/0
BGPR	2001:7::/64	0	187	IP64/0
BGPR	2001:9::/64	0	200	IP64/0
BGPR	2001:17::/64	0	200	IP64/0
Dir*	2002:2::/64	1	7889	Eth/1
RIP6	2002:5::/64	3	10	FE80::220:35FF:FE45:2488 Eth/1
RIP6	2002:6::/64	2	10	FE80::220:35FF:FE45:2488 Eth/1
RIP6	2002:9::/64	2	10	FE80::220:35FF:FE45:2488 Eth/1
RIP6	2002:99::/64	3	10	FE80::220:35FF:FE45:2488 Eth/1
RIP6	2002:1111::/64	3	10	FE80::220:35FF:FE45:2488 Eth/1
Dir*	2003:1::/64	1	7889	IP64/0

IPv6 Routing table size: 768 nets (79872 bytes), 11 nets known
0 nets hidden, 0 nets deleted, 1 nets inactive
0 routes used internally, 756 routes free

Enable Neighbor

Use el mandato **enable neighbor** para habilitar un vecino específico o para habilitar todos los vecinos que se han inhabilitado. Este mandato inicia la sesión BGP6 con un vecino.

Sintaxis:

enable neighbor *dirección IPv6 vecino*

Ejemplo:

```
Enter a Neighbor address or :: for all neighbors []? ::  
neighbor 2003:1::6105 enabled
```

List

Use el mandato **list** para volcar todas las entradas de la tabla de direccionamiento de BGP6 o para visualizar información en rutas que se han anunciado a direcciones de vecino BGP6 especificadas (destinos) o de las que se han recibido dichas direcciones.

Sintaxis:

list all
dst_network *dirección red*
rt_rcved_from_nbr *dirección red*
rt_sent_to_nbr *dirección red*

all**Ejemplo:**

```

BGP6> list all

MED   Weight LPref AAG AGRAS ORG AS-Path

0     0     0     No 0     IGP seq[2001]
Network/Prefixlen: 2001:6::/64
Next Hop:          2003:1::6105
Next Hop LLA:      FE80::3030:30FF:FE30:B

0     0     0     No 0     IGP seq[2001]
Network/Prefixlen: 2001:7::/64
Next Hop:          2003:1::6105
Next Hop LLA:      FE80::3030:30FF:FE30:B

0     0     0     No 0     IGP seq[2001]
Network/Prefixlen: 2001:9::/64
Next Hop:          2003:1::6105
Next Hop LLA:      FE80::3030:30FF:FE30:B

0     0     0     No 0     IGP seq[2001]
Network/Prefixlen: 2001:17::/64
Next Hop:          2003:1::6105
Next Hop LLA:      FE80::3030:30FF:FE30:B

0     0     0     No 0     IGP
Network/Prefixlen: 2002:2::/64
Next Hop:          2002:2::6202
Next Hop LLA:      ::

0     0     0     No 0     IGP
Network/Prefixlen: 2002:5::/64
Next Hop:          2002:2::6202
Next Hop LLA:      ::

0     0     0     No 0     IGP
Network/Prefixlen: 2002:6::/64
Next Hop:          2002:2::6202
Next Hop LLA:      ::

0     0     0     No 0     IGP
Network/Prefixlen: 2002:9::/64
Next Hop:          2002:2::6202
Next Hop LLA:      ::

0     0     0     No 0     IGP
Network/Prefixlen: 2002:99::/64
Next Hop:          2002:2::6202
Next Hop LLA:      ::

0     0     0     No 0     IGP
Network/Prefixlen: 2002:1111::/64
Next Hop:          2002:2::6202
Next Hop LLA:      ::

```

dst_network dirección red

Muestra información detallada acerca de la red de destino o ruta especificada. El mandato muestra cómo se ha conocido una ruta específica, la mejor vía de acceso a un destino específico, la métrica asociada con la ruta y demás información.

Ejemplo:

Mandatos de supervisión de BGP6 (Talk 5)

```
BGP6>list dst_network
Destination network prefix []? 2002:1111::
Do you want specify prefix len? [No]: y
Prefix len (0-128) [64]?

Destination: 2002:1111::/64
Age:30, Upd#:4, LastSent: 0002:10:17

Eligible paths: 1
PathID: 0 - (Best Path)
ASpath:
Origin: IGP, Pref: 0, LocalPref: 0
Metric: 0, Weight: 0, MED: 0
NextHop: 2002:2::6202
NextHop LLA: ::
Neighbor: 2002:2::6202
AtomicAggr: No
```

ASpath Enumeración de los sistemas autónomos a los largo de la vía de acceso.

-seq: Secuencia de sistemas autónomos en orden en la vía de acceso

-set: Conjunto de sistemas autónomos en la vía de acceso.

Origin El que ha originado el destino. Es decir, EGP, IGP o Incomplete (originado por algún otro medio no conocido).

LocalPref Grado de preferencia para el destino por parte del direccionador originario.

Metric La métrica de vía de acceso con la que se importa la ruta.

Weight Peso de la vía de acceso.

MED Valor discriminador de varias salidas, que se utiliza para discriminar entre varios puntos de entrada/salida del mismo AS.

NextHop Dirección del direccionador a utilizar como dirección de reenvío para destinos alcanzables a través de la vía de acceso proporcionada.

AtomicAggr Indica si el direccionador que anuncia la vía de acceso ha incluido la vía de acceso en un atomic-aggregate.

rt_rcved_from_nbr *dirección red*

Lista todas las rutas recibidas del vecino BGP especificado.

Ejemplo:

```

BGP6>list rt_rcved_from_nbr
BGP6 neighbor address []? 2003:1::6105

Destinations obtained from BGP6 neighbor 2003:1::6105

MED  Weight LPref AAG AGRAS ORG AS-Path

0 0 0 No 0 IGP seq[2001]
Network/Prefixlen: 2001:9::/64
Next Hop: 2003:1::6105
Next Hop LLA: FE80::3030:30FF:FE30:B

0 0 0 No 0 IGP seq[2001]
Network/Prefixlen: 2001:7::/64
Next Hop: 2003:1::6105
Next Hop LLA: FE80::3030:30FF:FE30:B

0 0 0 No 0 IGP seq[2001]
Network/Prefixlen: 2001:17::/64
Next Hop: 2003:1::6105
Next Hop LLA: FE80::3030:30FF:FE30:B

0 0 0 No 0 IGP seq[2001]
Network/Prefixlen: 2001:6::/64
Next Hop: 2003:1::6105
Next Hop LLA: FE80::3030:30FF:FE30:B

```

rt_sent_to_nbr *dirección red*

Lista todas las rutas anunciadas al vecino BGP especificado.

Ejemplo:

```

BGP6>list rt_sent_to_nbr
BGP6 neighbor address []? 2003:1::6105

Destinations advertised to BGP6 neighbor 2003:1::6105

MED  Weight LPref AAG AGRAS ORG AS-Path

0 0 0 No 0 IGP
Network/Prefixlen: 2002:9::/64
Next Hop: 2002:2::6202
Next Hop LLA: ::

0 0 0 No 0 IGP
Network/Prefixlen: 2002:5::/64
Next Hop: 2002:2::6202
Next Hop LLA: ::

0 0 0 No 0 IGP
Network/Prefixlen: 2002:99::/64
Next Hop: 2002:2::6202
Next Hop LLA: ::

0 0 0 No 0 IGP
Network/Prefixlen: 2002:1111::/64
Next Hop: 2002:2::6202
Next Hop LLA: ::

0 0 0 No 0 IGP
Network/Prefixlen: 2002:6::/64
Next Hop: 2002:2::6202
Next Hop LLA: ::

```

Neighbors

Use el mandato **neighbors** para visualizar información acerca de todos los vecinos BGP6 activos.

Sintaxis:

neighbors *dirección IPv6 vecino*

Ejemplo:

Mandatos de supervisión de BGP6 (Talk 5)

BGP6>neighbors

Address:	2003:1::6105	Status	State	DAY-HH:MM:SS	AS	Upd#
bgp6-ID:	20.1.7.5	ENABLD	Established	000-00:03:42	2001	11

IPv6-Address

Especifica la dirección IPv6 del vecino BGP6.

State Especifica el estado de la conexión. Los estados posibles son:

Connect Esperando que se complete la conexión TCP con el vecino.

Active En caso de producirse una anomalía de la conexión TCP, el estado cambia a activo y el intento de llegar al vecino continúa.

OpenSent En este estado se ha enviado OPEN y BGP6 espera un mensaje OPEN del vecino.

OpenConfirm En este estado se ha enviado KEEPALIVE como respuesta al mensaje OPEN del vecino, y espera una notificación KEEPALIVE del vecino.

Established Se ha establecido satisfactoriamente una conexión BGP6 y ahora puede empezar a intercambiar mensajes UPDATE.

BGP-ID Especifica el número de identificación BGP6 del vecino.

AS Especifica el número de AS del vecino.

Upd# Especifica el número de secuencia del último mensaje UPDATE enviado al vecino.

IPv6 neighbor address

Use el mandato **neighbor** para visualizar datos detallados de un vecino BGP6 específico.

Ejemplo:

```
BGP6>neighbors 2000::662:0
Active Conn: None
Passve Conn: Sprt:179 Dprt:1026 State: Established KeepAlive/Hold Time: 30/90
TCP connection errors: 1 TCP state transitions: 1

BGP6 Messages: Sent Received Sent Received
Open: 2 2 Update: 2 2
Notification: 1 0 KeepAlive: 2 2
Total Messages: 7 6

Msg Header Errs: Sent Received Sent Received
Conn sync err: 0 0 Bad msg length: 0 0
Bad msg type: 0 0

Open Msg Errs: Sent Received Sent Received
Unsupp versions: 0 0 Unsupp auth code: 0 0
Bad peer AS ident: 0 0 Auth failure: 0 0
Bad BGP ident: 0 0 Bad hold time: 0 0

Update Msg Errs: Sent Received Sent Received
Bad attr list: 0 0 AS routing loop: 0 0
Bad wlnk attr: 0 0 Bad NEXT_HOP atr: 0 0
Mssng wlnk attr: 0 0 Optional atr err: 0 0
Attr flags err: 0 0 Bad netwrk field: 0 0
Attr length err: 0 0 Bad AS_PATH attr: 0 0
Bad ORIGIN attr: 0 0

Total Errors: Sent Received Sent Received
Msg Header Errs: 0 0 Hold Timer Exprd: 0 0
Open Msg Errs: 0 0 FSM Errs: 0 0
Update Msg Errs: 0 0 Cease: 1 0
```

Parameter

Use el mandato **parameter** de BGP6 para visualizar los valores globales BGP6 instalados en el sistema BGP6.

Sintaxis:

parameter

Ejemplo:

```
compare-med-from-diff-as is disabled.
IPv6-route-table-scan-timer value is 1 seconds.
```

Paths

Use el mandato **paths** de BGP6 para visualizar las vías de acceso almacenadas en la base de datos de descripción de la vía de acceso.

Sintaxis:

paths

Ejemplo:

```
paths
PathId MED   AAG AGRAS RefCnt ORG AS_PATH

0      0      No 0      6      IGP
Next Hop:    2002:2::6202
Next Hop LLA: ::

1      0      No 0      2      IGP seq[2001]
Next Hop:    2003:1::6105
Next Hop LLA: FE80::3030:30FF:FE30:B

2      0      No 0      2      IGP seq[2001]
Next Hop:    2003:1::6105
Next Hop LLA: FE80::3030:30FF:FE30:B
```

- PathId** Identificador de vía de acceso
- NextHop** Dirección del direccionador a utilizar como dirección de reenvío para los destinos que pueden alcanzarse a través de la vía de acceso proporcionada.
- MED** Discriminador de varias salidas que se utiliza para discriminar entre varios puntos de entrada/salida del mismo AS.
- AAG** Indica si en la vía de acceso se ha efectuado atomic-aggregate, es decir, el direccionador que está anunciando la vía de acceso proporcionada ha seleccionado la ruta menos específica por encima de la más específica cuando se le han presentado rutas solapadas.
- AGRAS** Indica el número de AS del hablante BGP6 que ha agregado las rutas.
- RefCnt** Indica el número de entidades de vía de acceso que hacen referencia al descriptor.
- ORG** Especifica qué ha originado los destinos anunciados en la vía de acceso proporcionada: EGP, IGP o Incomplete (originado por algún otro medio no conocido).

Mandatos de supervisión de BGP6 (Talk 5)

AS Path Enumeración de los sistemas autónomos a los largo de la vía de acceso.

seq: Secuencia de sistemas autónomos en orden en la vía de acceso.

set: Conjunto de sistemas autónomos en la vía de acceso.

Ping6

Si desea ver una explicación del mandato **ping6**, consulte “Ping6” en la página 502.

Policy-List

Use el mandato **policy-list** para visualizar la política instalada actualmente para estadísticas de uso y un vecino específico de cada política.

Ejemplo:

```
BGP6>policy-list
```

```
Destination network prefix []? 2003:1::6105
```

```
Policy Type (Receive/Send/Origin) [All]?
```

```
Receive policy list for all neighbors:
```

Idx	T	Match	OrgAS	AdjAS	IGPmet	Usage	Prefix
1	I	Range	0	0	0	5	2001::/16

```
AS-PATH with following ASs will be discarded:
```

```
Send policy list for all neighbor:
```

Idx	T	Match	TAG	AdjAS	Usage	Prefix
1	I	Range	0	0	11	2002::/16

```
Origin policy list for all neighbor:
```

Idx	T	Match	Tag	Usage	Prefix
1	I	Range	0	6	2002::/16

```
BGP6>policy-list
```

```
Neighbor address []? 2000::1
```

```
Policy Type (Receive/Send/Origin) [All]? r
```

```
Receive policy list for neighbor '2000::1' :
```

Idx	T	Match	OrgAS	AnyAS	MED	Weight	LPref	IGPmet	Usage	Prefix
1	I	Range	0	0	10	0	100	0	0	::/0

```
BGP6>policy-list
```

```
Neighbor address []? 2000::1
```

```
Policy Type (Receive/Send/Origin) [All]? s
```

```
Send policy list for neighbor '2000::1' :
```

Idx	T	Match	OrgAS	AnyAS	Tag	MED	ASpad	Usage	Prefix
1	I	Range	0	0	0	30	0	0	::/0

```
BGP6>policy-list
```

```
Neighbor address []? 2000::1
```

```
Policy Type (Receive/Send/Origin) [All]? o
```

```
Origin policy list for all neighbor:
```

Idx	T	Match	Tag	Usage	Prefix
1	I	Range	0	2	::/0

Reset Neighbor

Use el mandato **reset neighbor** para restablecer el vecino BGP6 especificado, en base a los parámetros de configuración del vecino almacenados en la memoria de configuración.

Sintaxis:

reset neighbor *dirección IPv6 vecino*

Ejemplo: **reset neighbor**

```
Enter a Neighbor address: []? 2003:1::6105
resetting neighbor 2003:1::6105
```

Sizes

Use el mandato **sizes** de BGP6 para visualizar el número de entradas almacenadas en las diversas bases de datos.

Sintaxis:

sizes

Ejemplo: **sizes**

```
# Paths: 10
# Path descriptors: 3
# Update sequence#: 11
# Routing tbl entries (allocated): 10
# Current tbl entries (not imported): 0
# Current tbl entries (imported to IGP): 4
```

Paths Número total de vías elegibles para todas las rutas de la tabla de direccionamiento de BGP6.

Path descriptors

Número total de descriptores de vía de acceso en la base de datos utilizada para retener información de vía de acceso común.

Update sequence#

Indica el número de secuencia de actualización actual.

Routing tbl entries (allocated)

Indica el número de entradas de la tabla de direccionamiento de BGP6.

Current tbl entries (not imported)

Indica el número de rutas BGP6 no importadas a IGP.

Current tbl entries(imported to IGP)

Indica el número de rutas BGP6 importadas a IGP.

Traceroute6

Si desea obtener una explicación del mandato **traceroute6**, consulte la sección "Traceroute6" en la página 503.

Soporte de reconfiguración dinámica de BGP6

Esta sección describe la reconfiguración dinámica (DR) en la medida en que afecta a los mandatos de Talk 6 y Talk 5.

Delete Interface de CONFIG (Talk 6)(Suprimir interfaz)

Border Gateway Protocol para IPv6 (BGP6) da soporte al mandato **delete interface** de CONFIG (Talk 6), teniendo en cuenta lo siguiente:

Suprime vecinos externos BGP6 configurados si la dirección de vecino tiene un prefijo IPv6 común con una dirección IPv6 suprimida en dicha interfaz.

Activate Interface de GWCON (Talk 5)(Activar interfaz)

El mandato **activate interface** de GWCON (Talk 5) no es aplicable para BGP6. BGP6 no tiene registros de SRAM asociados con una interfaz.

Reset Interface de GWCON (Talk 5)(Restablecer interfaz)

El mandato de GWCON (Talk 5) **reset interface** no es aplicable para BGP6. BGP6 no tiene registros de SRAM asociados con una interfaz.

Mandatos Component Reset de GWCON (Talk 5)(Restablecer componente)

BGP6 da soporte a los siguientes mandatos **reset** de GWCON (Talk 5) específicos de BGP6:

Mandato GWCON, Protocol Bgp6, Reset Neighbor

Descripción: Añade o suprime un vecino BGP6. Cambia las políticas y parámetros de vecino.

Efecto en la red: La conexión de vecino BGP6 y las rutas conocidas se actualizan en base a los cambios efectuados en la configuración.

Limitaciones: Ninguna.

La tabla siguiente resume los cambios de configuración de BGP6 que se activan cuando se invoca el mandato **GWCON, protocol bgp6, reset neighbor**:

Mandatos cuyos cambios se activan con el mandato GWCON, protocol bgp6, reset neighbor
CONFIG, protocol BGP6, add neighbor
CONFIG, protocol BGP6, change neighbor
CONFIG, protocol BGP6, delete neighbor
CONFIG, protocol BGP6, attach policy-to-neighbor
CONFIG, protocol BGP6, change policy-to-neighbor
CONFIG, protocol BGP6, delete policy-to-neighbor
CONFIG, protocol BGP6, add policy-list
CONFIG, protocol BGP6, update policy-list

Mandatos de cambio temporal de GWCON (Talk 5)

BGP6 da soporte a los siguientes mandatos de 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 cualquier mandato reconfigurable dinámicamente.

Mandatos
GWCON, protocol BGP6, enable neighbor
GWCON, protocol BGP6, disable neighbor

Mandatos no reconfigurables dinámicamente

La tabla siguiente describe los mandatos de configuración de BGP6 que no se pueden cambiar dinámicamente. Para activar estos mandatos, es necesario volver a cargar o reiniciar el dispositivo.

Mandatos
CONFIG, protocol BGP6, enable bgp6
CONFIG, protocol BGP6, disable bgp6
CONFIG, protocol BGP6, add no-receive
CONFIG, protocol BGP6, delete no-receive
CONFIG, protocol BGP6, add/change/delete/move aggregate
CONFIG, protocol BGP6, add/change/delete/move originate-policy
CONFIG, protocol BGP6, add/change/delete/move receive-policy
CONFIG, protocol BGP6, add/change/delete/move send-policy
CONFIG, protocol BGP6, enable compare-med-from-diff-as
CONFIG, protocol BGP6, set ipv6-route-table-scan-timer

Apéndice A. Comparación de protocolos

Este apéndice compara algunos de los protocolos más conocidos a los que da soporte el direccionador. Se proporciona como guía de ayuda y su objetivo no es servir de consulta.

Tabla de comparación de los protocolos

La tabla siguiente compara los protocolos.

Modelo OSI de ISO	TCP/IP	IPX	Otros
7 Aplicación 6 Presentación 5 Sesión	Telnet, FTP, TFTP, SGMP		
4 Transporte	TCP, UDP	PXP, SPX	
3 Red	IP, RIP, BGP, ICMP	RIP, SAP	
2 Enlace de datos	Red local		HDLC
1 Física			

Clave para los protocolos

La Tabla 125 es una clave para los protocolos.

Protocolo	Descripción
BGP	Border Gateway Protocol. Protocolo de direccionamiento externo IP.
FTP, TFTP	File Transfer Protocol; Trivial File Transfer Protocol.
ICMP	Internet Control Message Protocol. Se usa para enviar mensajes de control y de error de nivel de red entre direccionadores y sistemas principales.
IP	Internet protocol. IP es un protocolo de transporte estándar de uso muy extendido. IP es el protocolo básico de los direccionadores 2210. IP deja una parte de la comprobación de errores a los protocolos de nivel superior (de extremo a extremo).
IPX	Internet Packet Exchange Protocol.
RIP	Routing Information Protocol (Los protocolos de direccionamiento se usan para determinar los recorridos de los datos y la topología de la red). RIP es el protocolo de direccionamiento de IP más difundido.
SGMP	Simple Gateway Monitoring Protocol. Se usa para obtener estadísticas en forma legible por máquina de los direccionadores 2210.
SNMP	Simple Network Management Protocol. Se usa para obtener estadísticas en forma legible por la máquina de direccionadores 2210.

Comparación de protocolos

<i>Tabla 125 (Página 2 de 2). Clave para los protocolos</i>	
Protocolo	Descripción
TCP	Transport Control Protocol. Protocolo de extremo a extremo (sistema principal a sistema principal) utilizado con frecuencia con IP. Es útil para enviar flujos de datos. Usa sumas de comprobación, reconocimientos y tiempos de espera para asegurarse de la entrega correcta de todas las secuencias de datos.

Apéndice B. Tamaños de los paquetes

Este apéndice trata los tamaños de los paquetes para los diferentes protocolos y redes con soporte. Está formado por las secciones siguientes:

- Cuestiones generales
- Límites de tamaño específicos de la red
- Límites de tamaño específicos del protocolo
- Cambio de los tamaños máximos de paquete

Cuestiones generales

Como información general para el objetivo de la presente discusión, los paquetes que manejan los direccionadores están formados por datos del usuario e información de cabecera.

La cantidad de datos del usuario contenidos en el paquete está limitada por la cantidad de información de cabecera de dicho paquete. Esta cantidad de información depende (como mínimo):

- De los tipos de red sobre los que debe viajar el paquete.
- De los protocolos que usan las redes.

Los factores siguientes influyen en el tamaño del contenido del paquete:

- Longitud de la información de la cabecera de enlace de datos que el tipo de red y la interfaz actuales necesitan que tenga el paquete.
- Longitud de la información final (si la hay) que el tipo de red y la interfaz actuales necesitan que tenga el paquete.

En cualquier red, la suma del tamaño máximo de los datos junto con el tamaño de la cabecera y el de la información final es igual al tamaño máximo del paquete de la red. Cuando se direcciona entre redes cuyo tamaño máximo de paquete sea diferente, se producirá una fragmentación de éste.

Límites de tamaño específicos de la red

Teniendo en cuenta la información proporcionada en la sección anterior, es posible determinar la cantidad máxima de datos de la capa de la red que tiene soporte de cada capa de enlace de datos (interfaz de la red). La Tabla 126 lista los tamaños máximos de los paquetes por omisión para los tipos de interfaz comunes.

<i>Tabla 126 (Página 1 de 2). Tamaño máximo por omisión del paquete específico de red</i>			
Tipo de red (enlace de datos)	Tamaño máximo del paquete de la capa de red (bytes)	Longitud de la cabecera de red	Parte final de la infor- mación
Red en anillo 4 Mbps	2052	22	0

Tamaños de los paquetes

Tabla 126 (Página 2 de 2). Tamaño máximo por omisión del paquete específico de red

Tipo de red (enlace de datos)	Tamaño máximo del paquete de la capa de red (bytes)	Longitud de la cabecera de red	Parte final de la información
Red en anillo 16 Mbps	2052	22	0
Ethernet	1500	18	4
PPP	2046	2	0
Frame Relay	2048 (ver notas)	variable	2

Nota: Para las interfaces de Frame Relay se configura el tamaño de trama máximo y no el tamaño máximo del paquete de la capa de red. Para determinar el tamaño máximo del paquete de la capa de la red para un protocolo, consulte la descripción del mandato **set frame-size** en el capítulo titulado *Configuring and Monitoring Frame Relay Interfaces (Configuración y supervisión de interfaces de Frame Relay)* en el manual *Guía del usuario de software*.

Nota: Puede cambiar el tamaño máximo del paquete para las interfaces que no sean Ethernet. Use el mandato **network** en el indicador `Config>` para acceder a los mandatos de configuración de la interfaz.

El tamaño máximo del paquete es la cantidad máxima de datos que el reenviador de protocolos puede pasar al dispositivo.

Nota: Estos números corresponden a las MTU de 4.2 BSD UNIX.

Para un paquete IP, esto incluye la cabecera de IP, la cabecera de UDP o TCP y todos los datos.

El tamaño del paquete que se está usando se muestra cuando se usa el mandato de memoria `GWCON` del direccionador. El tamaño "Pkt" es el tamaño del paquete de la capa de red. Los tamaños de Hdr (cabecera) y Tlr (parte final) dependen de las redes y de sus respectivas interfaces de red.

Límites de tamaño específicos del protocolo

Esta sección explica los límites de tamaño específicos de los protocolos.

Longitudes de paquete IP

Las especificaciones del protocolo IP no necesitan una implementación de IP en el sistema principal para aceptar paquetes IP de más de 576 octetos; no obstante, las implementaciones de IP del direccionador deben acomodar paquetes IP de cualquier longitud hasta los límites impuestos por los paquetes específicos de la red en uso.

Además, el IP del direccionador efectúa una fragmentación y ensambla de nuevo los paquetes de forma transparente y, de no ser así, superarían las restricciones de longitud específicas de la red, tal como están indicadas en la especificación de IP.

La falta de coincidencia del tamaño del paquete no produce problemas de conectividad. No obstante, el ensamblamiento de fragmentos perjudica el rendimiento, por lo que debe evitarse en la medida de lo posible la fragmentación.

Cambio de los tamaños máximos de paquete

Por lo general, el direccionador establece automáticamente el tamaño máximo del paquete de la capa de red en el tamaño de paquete más grande posible en todas las redes conectadas. A continuación, añade las cabeceras e información final necesarias para que las redes determinen el tamaño del almacenamiento intermedio interno, que es superior al tamaño de la capa de red.

Algunas redes (Red en anillo 4 Mbps y Red en anillo 16 Mbps) le permiten configurar tamaños de paquete máximos. La configuración de tamaños máximos de paquete influye en el tamaño de los almacenamientos intermedios usados en el direccionador y esto, a su vez, influye en el número de almacenamientos intermedios disponibles para un tamaño de memoria determinado. Los direccionadores determinan automáticamente qué tamaño va a necesitar el almacenamiento intermedio. Puede cambiar el tamaño de paquete máximo de la capa de red que el direccionador maneja usando el mandato `set packet-size`; no obstante, no use este mandato a menos que el servicio de atención al cliente se lo indique específicamente.

Tamaños de los paquetes

Apéndice C. 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 frontera 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	Oído y boca
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
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	Oficina de cambio extranjero
FXS	Estación de cambio extranjero
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
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
LSB	Bit menos significativo
LSI	Interfaz de métodos abreviados de LAN
LSreq	Solicitud 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	Difusión múltiple
MCF	Filtración 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 difusión múltiple
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
NBMA	Acceso múltiple sin difusión
NBP	Name Binding Protocol
NBR	Direccionador contiguo
NCP	Network Control Protocol
NCP	Network Core Protocol
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
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	Punto a punto
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	Solicitud de emisión
Rtype	Tipo de ruta
rxmits	Retransmisiones
rxmt	Retransmisión
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 sobre 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 petionario 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 solicitud 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 del release actual no modificado del programa.

asequibilidad. Capacidad de un nodo o recurso para comunicarse con otro nodo o recurso.

asíncrono (ASYNCR). 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 solicitud 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 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)

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 solicitud 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.

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. (I) (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. (I) (2) Sinónimo

con funcionamiento en modalidad de paquete. Véase también *conmutación del circuito*.

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. (1) (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 *difusión múltiple*.

difusión múltiple. (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.

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 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 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 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.

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 contienda utilizando la detección y deferencia de portadora y resuelve la contienda 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 dirigitable (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.

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 (MMLTG)* 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 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 de 8 bytes registrado por IBM que identifica de manera exclusiva a 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) Uso 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) Frontera compartida 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) Alternancia de dos o más operaciones o funciones a través del uso solapado de un recurso del sistema. (2) En transmisión de datos, la alternancia de 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 recursos de LAN desde una estación de trabajo central.

LE. Emulación de LAN. Norma del ATM Forum que da soporte a aplicaciones de legado de LAN sobre redes ATM.

LEC. Cliente de emulación de LAN. Componente de la emulación de LAN 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.

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*.

M

mandato ping. Mandato que envía un paquete de solicitud de 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. (l) (A) (2) Utilizar un patrón de caracteres para controlar la retención o eliminación de partes de otro patrón de caracteres. (l) (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.

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 (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).

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, PC (Personal Computer) de IBM 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 solicitud.

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 `ralvm7.vnet.ibm.com`, cada uno de los siguientes es un nombre de dominio:

- `ralvm7.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 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.

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 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 solicitud de llamada virtual o circuito virtual permanente.

paquete de solicitud 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 solicitud 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 resta-

blezca una llamada virtual o un circuito virtual permanente. En el paquete también puede especificarse la razón de la solicitud.

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.

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 que conectan una red de área local a otra red de área local o sistema principal que utiliza distintos protocolos de enlace lógico. (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.

punto. 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 punto reenvía una trama a otro punto basándose en la dirección del control del acceso al medio (MAC).

punto de ruta. Función de un programa de punto de IBM que permite que dos sistemas de punto utilicen un enlace de telecomunicaciones para conectar dos LAN. Cada sistema de punto se conecta directamente a una de las LAN y el enlace de telecomunicaciones conecta los dos sistemas de punto.

punto raíz. Punto que es la raíz de un árbol de expansión formado entre otros puntos activos de la red de funciones de punto. El punto raíz origina y transmite unidades de datos de protocolo de punto (BPDU) a otros puntos activos para mantener la topología de árbol de expansión. Es el punto con la prioridad superior de la red.

puntos paralelo. Par de puntos 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.

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 fun-

cionar 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) 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 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. Nor-

malmente, 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 solicitud que indica al receptor que devuelva una respuesta sólo si la solicitud 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 para red en anillo de IBM, el servidor que acepta mandatos del LAN Network Manager (LNM) para obtener información de estación, establecer parámetros de estación y eliminar estaciones del 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 la 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 para la Red en Anillo de IBM, servidor que mantiene información estadística sobre las 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 de salida. 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 excedidos 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 solicitud de 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. (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. (2) Unidad de transmisión en algunas redes de área local, incluyendo 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 solicitud/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 de 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 en 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.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).

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.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.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.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

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.

W

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

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

A

access-control
 Mandato de supervisión de IPv6 497
activate
 Mandato de supervisión de APPN 235
activate_new_config
 Mandato de configuración de APPN 217
add
 Mandato de configuración de actualización del filtro de paquetes de IPv6 492
 Mandato de configuración de AppleTalk Phase 2 294
 Mandato de configuración de APPN 154
 mandato de configuración de IPv6 476
 mandato de configuración de NDP 508
 Mandato de configuración de OSI 388
 Mandato de configuración de RIP6 538
 Mandato de configuración de VINES 317
Address Resolution Protocol (ARP)
 VINES 314
addresses
 Mandato de supervisión de OSI/DECnet V 416
algoritmo de reintento del DLUR 42
antes de configurar 37
aping
 Mandato de supervisión de APPN 235
AppleTalk Control Protocol
 para PPP 286
AppleTalk Phase 2
 configuración 285
 parámetros de red 286, 289
 parámetros del direccionador 285
 procedimientos de configuración básicos 285, 288
 supervisión 293
APPN 94
 supervisión 230
APPN (DLSw) 25
APPN, Red de conexiones BAN Frame Relay 46, 199, 200
atecho
 Mandato de supervisión de AppleTalk Phase 2 302
ATM
 Uso de APPN 71
ATM LAN Emulation
 configuración de DNA IV 329
ayuda
 mandato de consola 293

B

Border Gateway Protocol para IPv6--ver BGP6 577
Border Node
 lista de direccionamientos 210
 tabla de correlaciones de COS 214
Branch Extender 16, 19, 29, 182, 183, 184, 209, 210

C

cache
 Mandato de supervisión de AppleTalk Phase 2 303
 Mandato de supervisión de IPv6 497
Circuito permanente RDSI
 Uso de APPN 51
clear 397
 Mandato de supervisión de PIM 525
cnp-Stats
 Mandato de supervisión de OSI/DECnet V 417
conexiones, redes 14
configurable, Cola de alertas retenidas 22, 37, 153
configuración de TN3270 bajo APPN 94
configuración del servidor tn3270E 94
configuración, cambios, efecto en el direccionador 24
configuración, opciones 25
configuración, requisitos 25
contabilidad y nodos, estadísticas 41
COS 37
CoS mapping table 35
counters
 Mandato de supervisión de AppleTalk Phase 2 304
 Mandato de supervisión de IPv6 498
 Mandato de supervisión de VINES 322

CH

change
 Mandato de configuración de actualización del filtro de paquetes de IPv6 494
 mandato de configuración de IPv6 483
 mandato de configuración de NDP 510
 Mandato de configuración de RIP6 538
change metric
 Mandato de supervisión de OSI/DECnet V 416
change prefix-address 395

D

DDDLU 99
 Creación de LU en VTAM 99
 ejemplo de definición de PU de VTAM 100
 supresión de LU desde VTAM 100
 uso de Network Dispatcher con 100

- deactivate link
 - Mandato de supervisión de APPN 236
- deactivate LU
 - mandato de supervisión de TN3270E 272
- DECnet NCP
 - Véase NCP 327
- delete
 - Mandato de configuración de actualización del filtro de paquetes de IPv6 495
 - Mandato de configuración de AppleTalk Phase 2 295
 - Mandato de configuración de APPN 217
 - mandato de configuración de IPv6 483
 - mandato de configuración de NDP 512
 - Mandato de configuración de OSI 398
 - Mandato de configuración de PIM 519
 - Mandato de configuración de RIP6 540
 - Mandato de configuración de VINES 318
- dhcpcv6-relay
 - Mandato de supervisión de NDP 514
- Dial on Demand 54
- Digital Network Architecture (DNA) phase IV 327
- Direccionador de germinación
 - AppleTalk Phase 2 286, 289
- direccionadores del salto siguiente 443
- disable
 - Mandato de configuración de AppleTalk Phase 2 296
 - Mandato de configuración de APPN 119
 - mandato de configuración de IPv6 483
 - mandato de configuración de NDP 512
 - Mandato de configuración de OSI 400
 - Mandato de configuración de PIM 519
 - Mandato de configuración de RIP6 541
 - Mandato de configuración de VINES 318
- dispositivos de destino 443
- DLUR 10, 36, 42
- DNA IV
 - configuración
 - para X.25 342
 - configuración sobre ATM LAN Emulation 329
 - consideraciones y limitaciones especiales 328
 - control de acceso
 - configuración 333
 - excluyente 334
 - gestión de tráfico 332
 - incluyente 333
 - direccionador designado para 329
 - direccionadores de áreas
 - descripción 330
 - nivel 1 330
 - nivel 2 330
 - direccionamiento 329
 - 802.5 Token 328
 - descripción 328
 - Enlace de datos Ethernet 328
 - Enlace de datos X.25 329
- DNA IV (*continuación*)
 - filtros de direccionamiento de áreas 335
 - fusión de dominios 337
 - Network Control Program (NCP) 331
 - Véase NCP 327
 - parámetros de direccionamiento 330
 - Protocolo LAT 327
 - soporte de área 327
 - soporte MOP 327
 - tablas de direccionamiento 330
 - terminología y conceptos 328
- DNA V
 - Configuración de X.25
 - Cuenta 2 342
 - redes 340
- DNAV-info
 - Mandato de supervisión de OSI/DECnet V 419
- DSPU de VTAM 12
- dump
 - Mandato de supervisión de AppleTalk Phase 2 304
 - Mandato de supervisión de APPN 236
 - Mandato de supervisión de IPv6 498
 - Mandato de supervisión de NDP 514
 - Mandato de supervisión de PIM 524
 - Mandato de supervisión de RIP6 548
 - VINES 323
- dump routing tables
 - mandato de supervisión de BGP6 570

E

- el direccionador como punto de entrada 20
- enable
 - Mandato de configuración de AppleTalk Phase 2 297
 - Mandato de configuración de APPN 119
 - mandato de configuración de IPv6 484
 - mandato de configuración de NDP 512
 - Mandato de configuración de OSI 400
 - Mandato de configuración de PIM 519
 - Mandato de configuración de RIP6 542
 - Mandato de configuración de VINES 319
- enlace, listas de parámetros de nivel 50
- es-adjacencies
 - Mandato de supervisión de OSI/DECnet V 420
- es-is-stats
 - Mandato de supervisión de OSI/DECnet V 420
- esfera de control 21
- establecimiento de características de grupo de transmisión 37
- exit 294
 - mandato de consola 294
 - Mandato de supervisión de VINES 325
- Extended Border Node 17, 19
 - configuración 30
 - CoS mapping table 35

Extended Border Node (*continuación*)
 lista de direccionamientos 33
 requisitos de red 19
extensiones
 extensiones de información de la vía de
 acceso 444
 extensiones IBM privadas del proveedor 444
extensiones específicas de IBM
 NHRP 444

F

focal, punto 20, 37
funciones
 IP versión 6 (IPv6) 469

G

gestión de nodos de red 20
gestión del nodo de red direccionador 20

H

HIDLU 101
HPR 8, 36

I

implementación en el direccionador 4
implícito, punto focal 23, 207
interface
 Mandato de supervisión de AppleTalk Phase 2 305
 Mandato de supervisión de IPv6 498
 Mandato de supervisión de PIM 525
Interfaces de NHRP
 configuración 433
 supervisión 449
interfaz de atajos lane (LSI)
 NHRP 441
internal
 Mandato de supervisión de IPv6 499
IP
 tamaño del paquete 584
IPv6
 configuración 475
 uso 469
 visión general 469
is-adjacencies
 Mandato de supervisión de OSI/DECnet V 423
is-is-stats
 Mandato de supervisión de OSI/DECnet V 423

J

join
 Mandato de supervisión de PIM 526

L

l1-routes
 Mandato de supervisión de OSI/DECnet V 425
l1-Summary
 Mandato de supervisión de OSI/DECnet V 426
l1-Update
 Mandato de supervisión de OSI/DECnet V 427
l2-Routes
 Mandato de supervisión de OSI/DECnet V 425
l2-Summary
 Mandato de supervisión de OSI/DECnet V 427
l2-Update
 Mandato de supervisión de OSI/DECnet V 428
leave
 Mandato de supervisión de PIM 526
list
 Mandato de configuración de actualización del filtro
 de paquetes de IPv6 496
 Mandato de configuración de AppleTalk Phase
 2 299
 Mandato de configuración de APPN 217
 mandato de configuración de IPv6 484
 mandato de configuración de NDP 512
 Mandato de configuración de OSI 401
 Mandato de configuración de PIM 519
 Mandato de configuración de RIP6 544
 Mandato de configuración de VINES 319
 Mandato de supervisión de APPN 237
 Mandato de supervisión de NDP 514
 Mandato de supervisión de RIP6 548
 mandato de supervisión de TN3270E 272
lista de direccionamientos 33
listas de exclusiones 443
log
 Mandato de supervisión de APPN 261
LSI 441
 Véase también interfaz de atajos lane (LSI)
LU, lista de parámetros 51

M

mandato de ipv6 475
Mandato de NDP 507
Mandato de PIM 518
Mandato de RIP6 537
Mandatos de configuración de actualización del filtro de
paquetes de IPv6
 add 492
 change 494
 delete 495
 list 496
 move 495
Mandatos de configuración de AppleTalk Phase 2
 add 294
 delete 295

Mandatos de configuración de AppleTalk Phase 2 (*continuación*)

- disable 296
- enable 297
- list 299
- set 300

Mandatos de configuración de APPN

- activate_new_config 217
- add 154
- delete 217
- enable/disable 119
- list 217
- set 119
- TN3270 117

mandatos de configuración de BGP6 552, 558, 560, 562, 563

- add
 - aggregate 552
 - neighbor 553
 - no-receive 554
 - receive 556
 - send 557
- change
 - change originate 559
 - change receive 560
 - change send 560

- delete
 - aggregate 560
 - neighbor 560
 - no 561
 - originate 561
 - receive 561
 - send 561

- disable
 - BGP6 speaker 562
 - classless-bgp 562
 - neighbor 562
- enable 562
 - BGP6 speaker 562
 - compare-med-from-diff-AS 563
 - neighbor 563

- list
 - aggregate 563
 - all 563
 - BGP6 speaker 564
 - neighbor 564
 - no 564
 - originate 564
 - receive 565
 - send 565
- move 565
- policy-to-neighbor 559, 561, 565
- set 566
- update 566

Mandatos de configuración de DNA IV

- ayuda 346

Mandatos de configuración de DNA IV (*continuación*)

- define
 - acceso de módulos 353
 - direccionamiento de módulos 354
 - nodo 355

- definición
 - circuito 346
 - executor 350

- purge
 - acceso de módulos 356
 - direccionamiento de módulos 356

- show
 - área 356
 - nodo 358

- show/list
 - acceso de módulos 364
 - circuito 359
 - direccionamiento de módulos 364
 - executor 362

- zero
 - acceso de módulos 365
 - circuito 365
 - executor 365

Mandatos de configuración de IPv6

- add 476
- change 483
- delete 483
- disable 483
- enable 484
- list 484
- move 487
- resumen 475
- set 487
- update 491

Mandatos de configuración de NCP

- purge 355
- resumen 345
- set 356
- show 356
- show circuit 359
- zero 365

Mandatos de configuración de NDP

- add 508
- change 510
- delete 512
- disable 512
- enable 512
- list 512
- resumen 507
- set 513

Mandatos de configuración de NHRP 433

- acceso 449
- add 452
- advanced 450
- change 454
- delete 453

Mandatos de configuración de NHRP (*continuación*)

- disable 450
- enable 450
- list 450, 455
- resumen 449
- set 456

Mandatos de configuración de OSI

- add 388
- clear 397
- change prefix address 395
- delete 398
- disable 400
- enable 400
- list 401
- resumen 387
- set 408

Mandatos de configuración de PIM

- delete 519
- disable 519
- enable 519
- list 519
- resumen 518
- set 521

Mandatos de configuración de RIP6

- add 538
- change 538
- delete 540
- disable 541
- enable 542
- list 544
- resumen 537
- set 544

Mandatos de configuración de VINES 317

Mandatos de supervisión de AppleTalk Phase 2

- atecho 302
- cache 303
- clear counters 304
- counters 304
- dump 304
- interface 305

Mandatos de supervisión de APPN

- acceso 230
- activate 235
- aping 235
- deactivate link 236
- dump 236
- list 237
- log 261
- memory 266
- restart 271
- resumen 231
- rtp status 269
- rtp switchpath 269
- rtp test 270
- stop 271
- tn3270e 271

mandatos de supervisión de BGP

- destinos
- recibido 573

mandatos de supervisión de BGP6

- disable neighbor 569
- dump routing tables 570
- enable neighbor 570
- list 570
- neighbors 573
- parameter 575
- paths 575
- ping6 576
- policy-list 576
- reset neighbor 577
- sizes 577
- traceroute6 577

Mandatos de supervisión de DNA IV

- ayuda 346
- define
 - acceso de módulos 353
 - direccionamiento de módulos 354
 - nodo 355
- definición
 - circuito 346
 - executor 350
- purge
 - acceso de módulos 356
 - direccionamiento de módulos 356
- show
 - área 356
 - nodo 358
- show/list
 - acceso de módulos 364
 - circuito 359
 - direccionamiento 364
 - executor 362
- zero
 - acceso de módulos 365
 - circuito 365
 - executor 365
 - module_access 365

Mandatos de supervisión de IPv6

- acceso 496
- access-control 497
- cache 497
- counters 498
- dump 498
- interface 498
- internal 499
- mcast 499
- mld 499
- packet-filter 501
- path-mtu 502
- ping6 502
- reset 500
- resumen 496

Mandatos de supervisión de IPv6 (*continuación*)

- route 500
- sizes 500
- sniffer 501
- static 501
- traceroute6 503
- tunnels 504

Mandatos de supervisión de NCP

- purge 355
- resumen 345
- set 356
- show 356
- show circuit 359
- zero 365

Mandatos de supervisión de NDP

- acceso 513
- dhcpv6-relay 514
- dump 514
- list 514
- ping6 515
- resumen 514

Mandatos de supervisión de NHRP

- acceso 460
- lista 460

Mandatos de supervisión de OSI/DECnet V

- addresses 416
- clnp-stats 417
- change metric 416
- designated-router 419
- DNAV-info 419
- es-adjacencias 420
- es-is-stats 420
- is-adjacencias 423
- is-is-stats 423
- I1-routes 425
- I1-summary 426
- I1-update 427
- I2-routes 425
- I2-summary 427
- I2-update 428
- Mandato de supervisión de OSI/DECnet V 419
- ping-1139 429
- resumen 415
- route 429
- send (echo packet) 430
- subnets 430
- toggle (alias/no alias) 431
- traceroute 431

Mandatos de supervisión de PIM

- acceso 523
- clear 525
- dump 524
- interface 525
- join 526
- leave 526
- mcache 526

Mandatos de supervisión de PIM (*continuación*)

- mgroups 527
- mstats 527
- neighbor 529
- pim 530
- ping 531
- reset 531
- resumen 524
- summary pim 530
- traceroute 531
- variables 531

Mandatos de supervisión de RIP6

- acceso 547
- dump 548
- list 548
- ping6 548
- reset 548
- resumen 547
- traceroute6 548

mandatos de supervisión de TN3270E

- deactivate LU 272
- list 272

Mandatos de supervisión de VINES

- counters 322
- dump 323
- exit 325

Marcación bajo pedido

- Uso de APPN 54

mcache

- Mandato de supervisión de PIM 526

mcast

- Mandato de supervisión de IPv6 499

memory

- Mandato de supervisión de APPN 266

mensajes IS-IS

- mensajes hello de IS a IS 374
- punto a punto 375

mgroups

- Mandato de supervisión de PIM 527

mld

- Mandato de supervisión de IPv6 499

move

- Mandato de configuración de actualización del filtro de paquetes de IPv6 495
- mandato de configuración de IPv6 487

mstats

- Mandato de supervisión de PIM 527

Multicast Forwarding Cache - -ver MFC 534

N

NCP

- descripción 331

NDP

- configuración 507

- neighbor
 - Mandato de supervisión de PIM 529
- neighbor discovery protocol para IPv6--ver NDP6 515
- Network Control Protocols (NCP)
 - para interfaces PPP
 - AppleTalk Control Protocol 286
- Next Hop Resolution Protocol
 - Véase también NHRP
 - visión general 433
- NHRP 433
 - atajos LANE 441
 - beneficios 434
 - direccionadores del salto siguiente 443
 - dispositivos de destino 443
 - ejemplos
 - classical IP y ELAN mixtos 439
 - conmutadores de LAN 438
 - Direccionador de salida 440
 - entorno classic IP con dispositivos no capacitados para NHRP 436
 - entorno de classic IP 436
 - LAN emulation 437
 - implementación 440
 - atajos de direccionador a direccionador no permitidos 445
 - extensiones específicas de IBM 444
 - limitaciones 435
 - listas de exclusiones 443
 - virtual network interface (VNI) 441
- nodo, ajuste 40
- nodo, listas de parámetros de nivel 51
- nodos, tipos 1

O

- obtención de ayuda 293
- opcionales, funciones 7
- Open System Interconnection (OSI)
 - actualizaciones de estado de enlace de L1 376
 - actualizaciones de estado de enlace L2 377
 - actualizaciones de estados de enlaces 376
 - áreas IS-IS 372
 - áreas sinónimas 373
 - bases de datos de estados de enlaces 376
 - codificación de prefijos de direcciones 380, 381
 - contraseñas de autenticación 381
 - direccionadores IS L2 conectados 377
 - direccionadores IS L2 sin conectar 377
 - direccionamiento de L1 377
 - Direccionamiento de L2 378
 - Direccionamiento de NSAP 368
 - direccionamiento externo 379
 - direccionamiento interno 379
 - direcciones de difusión múltiple 370
 - direcciones de red 368
 - dominio IS-IS 372

Open System Interconnection (OSI) (continuación)

- estructura de direcciones de la red 368
- formato de direccionamiento IS-IS 369
 - AFI 380
 - dirección de área 369
 - formato de dirección 370
 - ID del sistema 369
 - IDI de longitud fija 380
 - IDI de longitud variable 380
 - no pseudonodo 376, 377
 - prefijos de dirección por omisión 381
 - pseudonodo 376, 377
 - punto a punto 375
 - selector 370
- IS designado 375
- mensaje L1 IIH 374
- mensajes hello de IS a IS 374, 375
- mensajes hello de sistema final 382
- mensajes hello IS 382
- Mensajes L2 IIH 375
- métrica de direccionamiento 378
- Network Entity Title (NET) 369
- parte de dominio inicial (IDP) 369
 - descripción 369
- parte específica del dominio (DSP) 369
- protocolo ES-IS 381
- protocolos que se ejecutan bajo 368
- pseudonodo 375
- sistema final (ES) 367
- sistema intermedio (IS) 367
- tablas de direccionamiento 377
- unidades de datos del protocolo de red (NPDU) 367

OSI

- configuración 384
- X.25 sobre OSI 390
- OSI/DECnet V
 - supervisión 387

P

- packet-filter
 - Mandato de supervisión de IPv6 501
- path-mtu
 - Mandato de supervisión de IPv6 502
- PIM
 - configuración 517
 - Mandato de supervisión de PIM 530
- ping
 - Mandato de supervisión de PIM 531
- ping-1139
 - Mandato de supervisión de OSI/DECnet V 429
- ping6
 - mandato de supervisión de BGP6 576
 - Mandato de supervisión de IPv6 502
 - Mandato de supervisión de NDP 515

ping6 (*continuación*)
 Mandato de supervisión de RIP6 548
 Point-to-Point Protocol (PPP)
 AppleTalk Control Protocol 286
 policy-list
 mandato de supervisión de BGP6 576
 protocolo CLNP 368
 protocolo de direccionamiento Protocol Independent
 Multicast--ver PIM 532
 protocolo de información de direccionamiento para
 IPv6--ver RIP6 549
 protocolo ES-IS 368
 descripción 381
 mensaje hello 382
 protocolo IS-IS
 áreas IS-IS 372
 descripción 371
 dominio IS-IS 372
 mensajes hello de IS a IS
 L1 374
 Mensajes hello de IS a IS (IIH)
 L2 375
 visión general 368
 Protocolo Local Area Terminal (LAT) 327
 protocolos
 BGP 581
 clave 581
 Digital Network Architecture (DNA) Phase IV 327
 FTP 581
 ICMP 581
 IP 581
 IPX 581
 RIP 581
 SGMP 581
 SNMP 581
 tabla de comparación 581
 TCP 582
 TFTP 581
 puerto, listas de parámetros de nivel 50
 puertos, tipos soportados 23

reconfiguración dinámica (*continuación*)
 servidor NHRP 467
 reconfiguración dinámica de APPN 283
 reconfiguración dinámica de BGP6 577
 reconfiguración dinámica de IPv6 504
 reconfiguración dinámica de MFC 534
 reconfiguración dinámica de MFC para IPv6 535
 reconfiguración dinámica de NDP6 515
 reconfiguración dinámica de PIM 532
 reconfiguración dinámica de PIM para IPv6 533
 reconfiguración dinámica de RIP6 549
 reconfiguración dinámica del servidor NHRP 467
 Red en anillo 4/16
 tamaño del paquete 584
 reset
 Mandato de supervisión de IPv6 500
 Mandato de supervisión de PIM 531
 Mandato de supervisión de RIP6 548
 restart
 Mandato de supervisión de APPN 271
 restricciones 45
 resumen
 Mandatos de configuración de NCP 345
 Mandatos de supervisión de NCP 345
 resumen de mandatos
 BGP 551, 568
 DNA IV 345
 reunión de datos de sesión intermedia 41
 RIP6
 configuración 537
 route
 Mandato de supervisión de IPv6 500
 Mandato de supervisión de OSI/DECnet V 429
 rtp status
 Mandato de supervisión de APPN 269
 rtp switchpath
 Mandato de supervisión de APPN 269
 rtp test
 Mandato de supervisión de APPN 270

R

rastreo 41
 rastreos 41
 RDSI, conexión permanente 51
 reconfiguración dinámica
 APPN 283
 BGP6 577
 IPv6 504
 MFC 534
 MFC para IPv6 535
 NDP6 515
 PIM 532
 PIM para IPv6 533
 RIP6 549

S

SDLC 73
 Uso de APPN 73
 send (Echo Packet)
 Mandato de supervisión de OSI/DECnet V 430
 servidor de TN3270E 90
 mandatos de configuración 218
 mandatos de supervisión 271
 Parámetros de configuración 218
 set
 Mandato de configuración de AppleTalk Phase
 2 300
 Mandato de configuración de APPN 119
 mandato de configuración de IPv6 487
 mandato de configuración de NDP 513

- set (*continuación*)
 - Mandato de configuración de OSI 408
 - Mandato de configuración de PIM 521
 - Mandato de configuración de RIP6 544
 - Mandato de configuración de VINES 320
- sizes
 - Mandato de supervisión de IPv6 500
- sniffer
 - Mandato de supervisión de IPv6 501
- SNMP, uso del direccionador como nodo gestionado por 22
- soportadas, unidades de mensajes 22
- soportadas, unidades de mensajes, alertas relacionadas con APPN 22
- Soporte de Enterprise Extender para HPR sobre IP 23
- static
 - Mandato de supervisión de IPv6 501
- stop
 - Mandato de supervisión de APPN 271
- subnets
 - Mandato de supervisión de OSI/DECnet V 430
- summary pim
 - Mandato de supervisión de PIM 530
- supervisión
 - APPN 230
 - Mandatos de supervisión de IPv6 496
 - Mandatos de supervisión de NDP 514
 - Mandatos de supervisión de PIM 524
 - Mandatos de supervisión de RIP6 547

T

- tablas de direccionamiento
 - mandato de vuelco de BGP6 570
- talk
 - mandato OPCON 230, 475, 496, 507, 513, 518, 523, 537, 547
- tamaño del paquete 583
- tamaño RU 40, 135
- TG, funciones 37
- TN3270 89
 - configuración del servidor tn3270E 94
 - qué es 89
- tn3270e
 - Mandato de supervisión de APPN 271
- TN3270E Server
 - Configuración, con el identificador de nodo local 114
 - configuración, uso de DLUR 110
 - configuraciones de ejemplo 109
 - correlación de clientes con LU 102
 - correlación de dirección IP y puerto 108
 - correlación de direcciones IP de cliente con LU/agrupaciones 104
 - correlación del puerto TCP del servidor con una agrupación 107

- TN3270E Server (*continuación*)
 - equilibrio de carga entre varias PU 108
- toggle (Alias/No Alias)
 - Mandato de supervisión de OSI/DECnet V 431
- topología Database Garbage Collection 22
- traceroute
 - Mandato de supervisión de OSI/DECnet V 431
 - Mandato de supervisión de PIM 531
- traceroute6
 - mandato de supervisión de BGP6 577
 - Mandato de supervisión de IPv6 503
 - Mandato de supervisión de RIP6 548
- transporte de datos 45
- tunnels
 - Mandato de supervisión de IPv6 504

U

- unidades de mensajes soportadas, alertas relacionadas con APPN 22
- update
 - mandato de configuración de IPv6 491
- uso del direccionador como nodo gestionado por SNMP 22

V

- V.25 bis 67
 - Uso de APPN 67
- V.34
 - Uso de APPN 68
- variables
 - Mandato de supervisión de PIM 531
- VINES 319
 - Address Resolution Protocol (ARP) 314
 - configuración 307
 - establecimiento del número de nodos cliente 320
 - habilitación de una interfaz 319
 - habilitación global 319
 - Implementación de RTP 313
 - inhabilitación de una interfaz 318
 - inhabilitación global 318
 - mandatos de supervisión 321
 - nodos cliente 307
 - nodos de servicio 307
 - procedimientos de configuración básicos 315
 - protocolos de capa de red 308
 - Address Resolution Protocol (ARP) 314
 - Internet Control Protocol (ICP) 313
 - Routing Update Protocol (RTP) 310
 - VINES IP 308
 - supervisión 317
 - tablas de direccionamiento 311
 - establecimiento del tamaño 321
 - vuelco 324
 - tablas de vecinos 312
 - establecimiento del tamaño 321

VINES (*continuación*)

tablas de vecinos (*continuación*)

vuelco 323

visión general 307

virtual network interface (VNI)

NHRP 441

VNI 441

Véase también virtual network interface (VNI)

W

WAN, redireccionamiento 58

WAN, restauración 65

Hoja de Comentarios

Nways Multiprotocol Routing Services
Manual de consulta de supervisión
y configuración de protocolos
Volumen 2 Versión 3.4

Número de Publicación SC10-3428-01

En general, ¿está Ud. satisfecho con la información de este libro?

	Muy satisfecho	Satisfecho	Normal	Insatisfecho	Muy insatisfecho
Satisfacción general	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

¿Cómo valora los siguientes aspectos de este libro?

	Muy bien	Bien	Acep- table	Insatisfecho	Muy insatisfecho
Organización	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Información completa y precisa	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Información fácil de encontrar	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Utilidad de las ilustraciones	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Claridad de la redacción	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Calidad de la edición	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Adaptación a los formatos, unidades, etc. del país	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Comentarios y sugerencias:

Nombre _____

Dirección _____

Compañía u Organización _____

Teléfono _____



Dóblese por la línea de puntos

Por favor no lo grape

Dóblese por la línea de puntos

PONER
EL
SELLO
AQUÍ

IBM, S.A.
National Language Solutions Center
Av. Diagonal, 571
08029 Barcelona
España

Dóblese por la línea de puntos

Por favor no lo grape

Dóblese por la línea de puntos



SC10-3428-01

