

Nways Multiprotocol Access Services



Características de utilización y configuración

Versión 3.3

Nways Multiprotocol Access Services



Características de utilización y configuración Versión 3.3

Nota

Antes de utilizar este documento, lea la información general que se encuentra en "Avisos" en la página xxi.

Primera edición (junio de 1999)

Este manual es la traducción del original inglés *Nways Multiprotocol Access Services Using and Configuring Features Version 3.3* (SC30-3993-01).

Esta edición se aplica a la Versión 3.3 de IBM Nways Multiprotocol Access Services y a todos los releases y modificaciones posteriores hasta que se indique lo contrario en ediciones o circulares nuevas.

Solicite las publicaciones al representante de IBM o a la sucursal de IBM que le atiende localmente. Las publicaciones no se almacenan en las direcciones indicadas 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:

IBM S.A.
National Language Solutions Center
Avda. Diagonal 571, Edificio "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	xxi
Aviso para los usuarios de versiones en línea de este manual	xxiii
Marcas registradas	xxv
Prefacio	xxvii
A quién va dirigido este manual	xxvii
Acerca del software	xxvii
Convenios utilizados en este manual	xxviii
Visión general de la biblioteca	xxix
Resumen de los cambios para la Biblioteca de software de IBM 2216	xxxi
Programa de utilidad de red	xxxii
Funciones de software soportadas por Network Utility	xxxii
Cómo obtener ayuda	xxxiv
Cómo salir de un entorno de nivel inferior	xxxiv
Utilización de la reserva de ancho de banda y puesta en cola por prioridad	1
Sistema de reserva de ancho de banda	1
Reserva de ancho de banda a través de Frame Relay	3
Soporte de colas	4
Elegibilidad de eliminación	4
Definiciones de circuito por omisión para la gestión de clases de tráfico	5
Configuración de BRS para la voz a través de Frame Relay	5
Sistema de colas de prioridad	6
Colas de prioridad sin reserva de ancho de banda	6
Configuración de clases de tráfico	7
BRS y filtrado	8
Filtrado y códigos de direcciones MAC	8
Filtrado de números de puerto TCP/UDP	9
Filtrado de bits TOS IPv4	9
Utilización del proceso de bits de precedencia de IP Versión 4 para el tráfico	
SNA en túneles seguros IP y fragmentos secundarios	10
Filtrado SNA y APPN para el tráfico con puente	11
Orden de precedencia del filtrado	12
Configuraciones de ejemplo	13
Utilización de definiciones de circuito por omisión para la gestión de clases	
de tráfico de circuitos Frame Relay	13
Configuración y supervisión de reserva de ancho de banda	25
Visión general de la configuración de la reserva de ancho de banda	25
Mandatos de configuración de reserva de ancho de banda	26
Activate-IP-precedence-filtering	31
Add-circuit-class	31
Add-class	31
Assign	33
Assign-circuit	37
Change-circuit-class	37
Change-class	37
Circuit	37

Clear-block	38
Create-super-class	39
Deactivate-IP-precedence-filtering	39
Deassign	39
Deassign-circuit	39
Default-circuit-class	40
Del-circuit-class	40
Default-class	40
Del-class	40
Disable	41
Disable-hpr-over-ip-port-numbers	41
Enable	41
Enable-hpr-over-ip-port-numbers	42
Interface	43
List	44
Queue-length	47
Set-circuit-defaults	48
Show	48
Tag	49
Untag	49
Use-circuit-defaults	50
Acceso al indicador de supervisión de la reserva de ancho de banda	50
Mandatos de supervisión de reserva de ancho de banda	51
Circuit	52
Clear	52
Clear-Circuit-Class	52
Counters	52
Counters-circuit-class	53
Interface	54
Last	54
Last-circuit-class	54
Utilización del filtrado MAC	55
Filtrado MAC y tráfico DLSw	55
Parámetros de filtrado MAC	56
Parámetros de los elementos de filtro	56
Parámetros de lista de filtros	56
Parámetros de filtro	57
Utilización de los códigos del filtrado MAC	57
Configuración y supervisión del filtrado MAC	59
Acceso al indicador de configuración de filtrado MAC	59
Mandatos de configuración del filtrado MAC	59
Attach	60
Create	60
Default	61
Delete	61
Detach	62
Disable	62
Enable	62
List	62
Move	63
Reinit	63
Set-Cache	63

Update	63
Submandatos de actualización	64
Add	64
Delete	65
List	66
Move	67
Set-Action	67
Acceso al indicador de supervisión de filtrado MAC	67
Mandatos de supervisión de filtrado MAC	67
Clear	68
Disable	68
Enable	69
List	69
Reinit	70
Utilización de Restauración de WAN	71
Visión general de Restauración de WAN, Redireccionamiento de WAN y Marcación en desbordamiento	71
Restauración de WAN	71
Redireccionamiento de WAN	72
Marcación en desbordamiento	73
Antes de empezar	73
Procedimiento de configuración para la Restauración de WAN	74
Configuración de circuito de marcación secundario	74
Configuración y supervisión de Restauración de WAN	77
Mandatos de configuración de Restauración de WAN, Redireccionamiento de WAN y Marcación en desbordamiento	77
Add	78
Disable	79
Enable	80
List	81
Remove	82
Set	83
Acceso al proceso de supervisión de la interfaz de Restauración de WAN	86
Mandatos de supervisión de la Restauración de WAN	86
Clear	86
Disable	87
Enable	88
Set	89
List	92
La característica Redireccionamiento de WAN	99
Visión general del Redireccionamiento de WAN	99
Marcación en desbordamiento	100
Configuración del Redireccionamiento de WAN	101
Ejemplo de configuración del Redireccionamiento de WAN	102
Utilización de la característica Network Dispatcher	107
Visión general de Network Dispatcher	107
Equilibrio del tráfico TCP y UDP mediante Network Dispatcher	108
Alta disponibilidad para Network Dispatcher	109
Detección de anomalías	110
Sincronización de bases de datos	111

Estrategia de recuperación	111
Entrada en función de IP	111
Configuración de Network Dispatcher	111
Pasos de la configuración	114
Utilización de Network Dispatcher con el servidor TN3270	119
Claves para la configuración	120
LU explícitas y Network Dispatcher	121
Utilización de Network Dispatcher con la Antememoria del servidor de la web	121
Utilización de Network Dispatcher con la Antememoria de eNetwork Host On-Demand Client	121
Utilización de Network Dispatcher con la Antememoria escalable de alta disponibilidad (SHAC)	121
Configuración y supervisión de la característica Network Dispatcher	125
Acceso a los mandatos de configuración de Network Dispatcher	125
Mandatos de configuración de Network Dispatcher	125
Add	126
Clear	133
Disable	133
Enable	134
List	135
Remove	136
Set	139
Acceso a los mandatos de supervisión de Network Dispatcher	145
Mandatos de supervisión de Network Dispatcher	145
List	145
Quiesce	147
Report	148
Status	149
Switchover	152
Unquiesce	152
Configuración y supervisión de la Antememoria de IBM eNetwork Host On-Demand Client	155
Configuración de la Antememoria de Host On-Demand Client	155
Acceso al entorno de configuración de la Antememoria de Host On-Demand Client	159
Mandatos de la Antememoria de Host On-Demand Client	159
Activate	160
Add	160
Delete	161
List	161
Modify	162
Acceso al entorno de supervisión de la Antememoria de Host On-Demand Client	163
Mandatos de supervisión de la Antememoria de On-Demand Client	163
Activate	164
Clear	165
Enable	165
Delete	165
Disable	166
List	166
Modify	168

Utilización de la Antememoria del servidor de la web	169
Visión general de la Antememoria del servidor de la web	169
Colocación en la antememoria	171
Utilización del Proxy HTTP	174
Antememoria escalable de alta disponibilidad	176
Visión general del gestor de control de antememoria externa	179
Tabla de dependencias	180
Protocolo de control de antememoria externa	181
Formatos de vector del Protocolo de control de antememoria externa (ECCP)	183
Configuración y supervisión de la Antememoria del servidor de la web	207
Configuración de la Antememoria del servidor de la web	207
Acceso al entorno de la Antememoria del servidor de la web	214
Mandatos de la Antememoria del servidor de la web	214
Activate	214
Add	215
Delete	215
List	216
Modify	217
Acceso al entorno de supervisión de la Antememoria del servidor de la web	221
Mandatos de supervisión de la Antememoria del servidor de la web	221
Activate	222
Clear	223
Enable	223
Delete	223
Disable	224
List	224
Modify	227
Configuración y supervisión del Subsistema de codificación	229
Configuración del Subsistema de codificación	229
List	230
Set	231
Supervisión del Subsistema de codificación	231
List	232
Configuración y supervisión de la compresión de datos	237
Visión general de la compresión de datos	237
Conceptos de la compresión de datos	237
Conceptos básicos de la compresión de datos	238
Consideraciones	240
Configuración y supervisión de la compresión de datos en enlaces PPP	243
Configuración de la compresión de datos en enlaces PPP	243
Supervisión de la compresión de datos en enlaces PPP	244
Configuración y supervisión de la compresión de datos en enlaces Frame Relay	245
Configuración de la compresión de datos en enlaces Frame Relay	245
Supervisión de la compresión de datos en enlaces Frame Relay	247
Ejemplo: Supervisión de la compresión en una interfaz o circuito Frame Relay	248
Utilización de la autenticación local o remota	251
Utilización de la Seguridad de autenticación, autorización y contabilidad (AAA)	251

¿Qué es la Seguridad AAA?	251
Utilización de PPP	252
Protocolos de seguridad PPP válidos	252
Utilización del inicio de sesión	253
Protocolos de seguridad de Inicio de sesión/Administración válidos	254
Utilización de túneles	254
Protocolos de seguridad de túnel válidos	255
Normas de las contraseñas	255
Explicación de los servidores de autenticación	256
Soporte de SecurID	256
Configuración de autenticación	259
Acceso al indicador de configuración de autenticación	259
Mandatos de configuración de autenticación	259
Disable	259
List	260
Login	261
Nets-info	263
Password-rules	263
PPP	265
Servers	267
Set	270
Tunnel	271
User-profiles	272
Utilización y configuración de protocolos de cifrado	279
Cifrado PPP utilizando el Protocolo de control de cifrado	279
Configuración del cifrado ECP para PPP	280
Supervisión del cifrado ECP para PPP	280
Cifrado punto a punto de Microsoft (MPPE)	281
Configuración de MPPE	281
Supervisión de MPPE	282
Configuración del cifrado en interfaces Frame Relay	282
Supervisión del cifrado en interfaces Frame Relay	283
Configuración y supervisión de la Calidad de los servicios (QoS)	285
Visión general de la Calidad de los servicios	285
Ventajas de QoS	285
Parámetros de configuración de QoS	286
Ancho de banda máximo reservado (max-reserved-bandwidth)	287
Tipo de tráfico (traffic-type)	287
Velocidad mayor de célula (peak-cell-rate)	287
Velocidad sostenida de célula (sustained-cell-rate)	288
Tamaño máximo de ráfaga (max-burst-size)	288
Clase de QoS (qos-class)	289
Validar PCR de VCC de mejor esfuerzo (validate-pcr-of-best-effort-vccs)	290
Negociar QoS (negotiate-qos)	290
Aceptar parámetros QoS de LECS (accept-qos-params-from-lecs)	291
Acceso al indicador de configuración de QoS	291
Mandatos de Calidad de los servicios	292
Mandatos de configuración de QoS de LE Client	292
List	293
Set	293
Remove	296

Mandatos de configuración de QoS de la interfaz ATM	297
List	297
Set	297
Remove	299
Acceso a los mandatos de supervisión de QoS	300
Mandatos de supervisión de Calidad de los servicios	300
Mandatos de supervisión de QoS de LE Client	301
List	301
Utilización de la característica de política	307
Visión general de la política	307
Decisión y aplicación de una política	307
Objetos de política	310
Interacción entre LDAP y la base de datos de políticas	315
Esquema de política	317
Reglas de generación	319
Ejemplos de configuración	320
Política de IPSec/ISAKMP con QOS	321
Política única de IPSec/ISAKMP	331
Eliminar todo el tráfico público (regla de filtro)	334
Configuración y habilitación del motor de búsqueda de política LDAP	338
Configuración y supervisión de la característica de política	343
Acceso al indicador de configuración de política	343
Mandatos de configuración de política	343
Add	344
Change	357
Copy	357
Delete	357
Disable	358
Enable	358
List	358
Mandatos de configuración del servidor de política LDAP	358
Disable LDAP	359
Enable LDAP	359
Set Default-Policy	359
Set LDAP	361
Set Refresh	362
Acceso al indicador de supervisión de política	363
Mandatos de supervisión de política	363
Disable	363
Enable	364
Reset	364
Search	364
Status	365
List	365
Test	366
Utilización de Seguridad de IP	367
Visión general de la Seguridad de IP	367
Utilización de túneles seguros	367
Conceptos de Seguridad de IP	368
Terminología de la Seguridad de IP	368
Cabecera de autenticación IP	370

Carga de seguridad de encapsulación IP	371
Utilización de AH y ESP	372
Asociaciones de seguridad	372
Modalidad de túnel y modalidad de transporte	372
Modalidad de túnel en túnel	375
Descubrimiento de Unidad de transmisión máxima de vía de acceso	375
Diagrama de una red con un túnel de seguridad IP	376
Utilización del Intercambio de claves de Internet	377
Fases del Intercambio de claves de Internet	378
Negociación de un túnel de seguridad de IP	379
Utilización de la infraestructura de clave pública	380
Configuración de PKI	380
Utilización de la seguridad de IP manual (IPv4)	385
Utilización de la seguridad de IP manual	385
Configuración y supervisión de la Seguridad de IP	387
Configuración del Intercambio de claves de Internet (IPv4)	387
Configuración de la Infraestructura de clave pública (IPv4)	388
Obtención de un certificado	388
Mandatos de configuración de la Infraestructura de clave pública	389
Add	389
Change	389
Delete	390
List	391
Configuración de la Seguridad de IP manual (IPv4)	392
Configuración de los algoritmos	392
Configuración de claves de cifrado	393
Acceso al entorno de configuración de la Seguridad de IP	393
Mandatos de la configuración manual de la Seguridad de IP	393
Add Tunnel	394
Change Tunnel	399
Delete Tunnel	399
Disable	399
Enable	400
List	401
Set	402
Configuración de un túnel manual (IPv4)	402
Configuración del túnel para el direccionador A	402
Configuración del túnel para el direccionador B	403
Ejemplo: configuración manual de un túnel de Seguridad de IP con ESP	403
Ejemplo: configuración manual de un túnel de seguridad de IP con ESP y ESP-NULL	404
Configuración de la Seguridad de IP manual (IPv6)	404
Configuración de los algoritmos	405
Configuración de claves de cifrado	405
Acceso al entorno de configuración de la Seguridad de IP	405
Mandatos de la configuración manual de la Seguridad de IP	406
Configuración de un túnel manual (IPv6)	406
Creación del túnel de Seguridad de IP para el direccionador A	406
Configuración de filtros de paquetes para el direccionador A	407
Configuración de las reglas de control de acceso de filtros de paquetes para el direccionador A	407
Restablecimiento de la Seguridad de IP y de IP en el direccionador A	408
Creación del túnel de Seguridad de IP para el direccionador B	408

Configuración de filtros de paquetes para el direccionador B	408
Configuración de las reglas de control de acceso de filtros de paquetes para el direccionador B	409
Restablecimiento de la Seguridad de IP y de IPv6 en el direccionador B	409
Ejemplo: configuración de un túnel de Seguridad de IP con ESP	409
Ejemplo: configuración de un túnel de Seguridad de IP con ESP y ESP-NULL	410
Supervisión de la Seguridad de IP manual (IPv4)	410
Acceso al entorno de Intercambio de claves de Internet	410
Mandatos de supervisión del Intercambio de claves de Internet	411
Acceso al entorno de la Infraestructura de clave pública (IPv4)	413
Mandatos de supervisión de la Infraestructura de clave pública	413
Acceso al entorno de supervisión de la Seguridad de IP (IPv4)	416
Mandatos de supervisión de la Seguridad de IP (IPv4)	416
Supervisión de la Seguridad de IP manual (IPv6)	423
Acceso al entorno de supervisión de la Seguridad de IP	423
Mandatos de supervisión de la Seguridad de IP (IPv6)	423
Utilización de la característica de Servicios diferenciados	425
Visión general de los Servicios diferenciados	425
Terminología de los Servicios diferenciados	428
Configuración de los Servicios diferenciados	428
Configuración y supervisión de la característica de Servicios diferenciados	431
Acceso al indicador de configuración de los Servicios diferenciados	431
Mandatos de configuración de los Servicios diferenciados	431
Delete	432
Disable	432
Enable	432
List	433
Set	434
Acceso al entorno de supervisión de los Servicios diferenciados	436
Mandatos de supervisión de los Servicios diferenciados	437
Clear	437
DScache	437
List	438
Utilización de Layer 2 Tunneling (L2TP, PPTP, L2F)	443
Visión general de L2TP	443
Términos de L2TP	443
Características soportadas	444
Consideraciones sobre tiempo	446
Consideraciones sobre LCP	446
Configuración de Layer 2 Tunneling	447
Configuración y supervisión de protocolos Layer 2 Tunneling	453
Acceso al indicador de configuración de la interfaz L2T	453
Mandatos de configuración de la interfaz L2 Tunneling	453
Disable	454
Enable	454
Encapsulator	454
List	454
Set	454

Acceso al indicador de configuración de la característica L2 Tunneling	455
Mandatos de configuración de la característica L2 Tunneling	455
Add	456
Disable	456
Enable	457
Encapsulator	458
List	458
Set	459
Acceso al indicador de supervisión de L2 Tunneling	460
Mandatos de supervisión de L2 Tunneling	461
Call	461
Kill	464
Memory	464
Start	465
Stop	465
Tunnel	465
Utilización de la conversión de direcciones de red	469
Conversión de puertos de direcciones de red	470
Correlaciones de direcciones estáticas	471
Correlaciones de direcciones estáticas NAT	471
Correlación de direcciones estáticas NAPT	471
Definición de filtros de paquetes y reglas de control de acceso para NAT	472
Ejemplo: Configuración de NAT con filtros IP y reglas de control de acceso	472
Configuración y supervisión de la Conversión de direcciones de red	477
Acceso al entorno de configuración de la Conversión de direcciones de red	477
Mandatos de configuración de la Conversión de direcciones de red	477
Change	478
Delete	478
Disable	479
Enable	479
List	479
Map	480
Reserve	481
Reset	483
Set	483
Translate	484
Acceso al entorno de supervisión de la Conversión de direcciones de red	484
Mandatos de supervisión de la Conversión de direcciones de red	484
List	485
Reset	486
Utilización de un Acceso de marcación de entrada a las LAN (DIALs)	
Server	487
Antes de utilizar Dial-In-Access	488
Configuración del acceso de marcación de entrada	488
Configuración de interfaces de marcación de entrada	488
Utilización de módem nulo	490
Antes de configurar los parámetros globales de DIAL	490
Direcciones IP proporcionadas por el servidor	490
DHCP (Dynamic Host Configuration Protocol)	492
Servidor de nombres de dominio dinámico (DDNS)	494

Configuración de DIAL	495
Acceso al entorno de configuración global de DIAL	495
Mandatos de configuración global de DIAL	495
Add	496
Delete	496
Disable	497
Enable	498
List	498
Set	500
Acceso al entorno de supervisión global de DIAL	503
Mandatos de supervisión global de DIAL	503
Clear	503
List	504
Reset	505
Utilización del servidor DHCP	507
Introducción a DHCP	507
Operación de DHCP	507
Renovación de alquileres	509
Movimiento de clientes	509
Modificación de las opciones del servidor	509
Número de servidores DHCP	510
Un único servidor DHCP	510
Múltiples servidores DHCP	510
Servidores BOOTP	511
Clientes DHCP especiales	511
Períodos de tiempo de alquiler	512
Conceptos y terminología	512
Servidor DHCP y parámetros de alquiler	515
Opciones de DHCP	515
Formatos de opción	515
Opciones básicas proporcionadas al cliente	517
Opciones de parámetros de capa IP por sistema principal	520
Opciones de parámetros de capa IP por interfaz	521
Opciones de parámetros de capa de enlace por interfaz	522
Opciones de parámetros de TCP	522
Opciones de parámetros de aplicaciones y servicios	522
Opciones de extensiones DHCP	524
Opciones específicas de IBM	528
Opciones de proveedor	528
Configuración de IP para DHCP	529
Adición de una dirección IP	529
Utilización de Simple-Internet-Access de IP	529
Configuración de ejemplo de servidor DHCP	530
Archivo de texto ASCII	530
Configuración de OPCON (Talk 6)	533
Configuración y supervisión del servidor DHCP	539
Acceso al entorno de configuración de servidor DHCP	539
Mandatos de configuración del servidor DHCP	539
Add	540
Change	546
Delete	551
Disable	555

Enable	555
List	556
Set	563
Acceso al entorno de supervisión de servidor DHCP	572
Mandatos de supervisión del servidor DHCP	573
Disable	573
Enable	573
List	573
Reset	574
Request	574
Utilización de la característica Thin Server	577
Visión general de la Network Station	577
Visión general de la característica Thin Server	578
Soporte de BootP/DHCP	579
Protocolos utilizados para establecer comunicación con las Network Stations	580
Utilización de RFS	580
Utilización de TFTP	580
Utilización de NFS	581
Actualizaciones de la antememoria de archivos	581
Configuración del entorno Thin Server	581
Recomendaciones sobre la configuración	582
Configuración del servidor BootP/DHCP	583
Configuración del servidor para el entorno Thin Server	583
Configuración de BootP Relay	583
Configuración de la dirección IP interna	584
Configuración del TSF	584
Configuración de ejemplo	584
Configuración del AS/400	585
Configuración del IBM 2216 (TSF)	586
Configuración y supervisión de la función Thin Server	591
Acceso al entorno de configuración de TSF	591
Mandatos de configuración de TSF	591
Add	592
Delete	597
List	598
Modify	598
Set	599
Acceso al entorno de supervisión de TSF	601
Mandatos de supervisión de TSF	601
Delete	601
Flush	602
List	602
Refresh	606
Reset	606
Restart	606
Set	607
Configuración y supervisión de VCRM	609
Acceso al entorno de configuración de VCRM	609
Acceso al entorno de supervisión de VCRM	609
Mandatos de supervisión de VCRM	610
Clear	610

Queue	610
Apéndice A. Atributos AAA remotos	613
Radius	613
Palabras clave	613
TACACS+	614
Apéndice B. Lista de Abreviaturas	617
Glosario	627
Índice	655

Figuras

1.	Relación entre la clase de tráfico BRS PPP y las colas de prioridad de las clases de tráfico	2
2.	Relación entre la clase de circuito BRS Frame Relay y las clases de tráfico	2
3.	Redireccionamiento de WAN	100
4.	Ejemplo de configuración del Redireccionamiento de WAN	102
5.	Ejemplo de Network Dispatcher configurado con un único cluster y 2 puertos	112
6.	Ejemplo de Network Dispatcher configurado con 3 clusters y 3 URL	113
7.	Ejemplo de Network Dispatcher configurado con 3 clusters y 3 puertos	114
8.	Configuración de Network Dispatcher de alta disponibilidad	115
9.	Dos antememorias con Network Dispatcher, cliente y servidor de fondo	123
10.	Network Dispatcher sin Antememoria del servidor de la web	170
11.	Network Dispatcher con Antememoria del servidor de la web y sin entradas en la antememoria	170
12.	Network Dispatcher con Antememoria del servidor de la web y con entradas en la antememoria	171
13.	Petición de antememoria encontrada	176
14.	Petición reenviada a la antememoria responsable	177
15.	Petición reenviada al servidor de fondo	178
16.	Petición reenviada a la antememoria responsable y no encontrada	178
17.	Vector de respuesta de mandato	184
18.	Formato de subvector	187
19.	Formato de subcampo	202
20.	Ejemplo de compresión de datos bidireccional con diccionarios de datos	240
21.	Ejemplo de configuración de la compresión en un enlace PPP	244
22.	Supervisión de la compresión en una interfaz PPP	245
23.	Ejemplo de configuración de la compresión en un enlace Frame Relay	246
24.	Nombre de usuario y código de paso de SecurID	256
25.	Código de paso de SecurID con la señal siguiente	256
26.	Flujo de paquetes IP y la base de datos de políticas	308
27.	Relación de objetos de configuración de política	315
28.	Seguridad del tráfico a través de Internet	317
29.	Estructura de esquema de política	318
30.	Configuración de IPSec/ISAKMP con QOS	321
31.	Configuración de IPSec y nueva utilización de una definición anterior	331
32.	Creación de un mensaje autenticado de HMAC MD5	371
33.	Formato de datagrama protegido por AH	373
34.	Formato de datagrama protegido por ESP	373
35.	Anidado de ESP en un túnel de AH	374
36.	Paquete L2TP protegido por IPSec	374
37.	Red con IPSec y NAT	377
38.	Vía de acceso de paquete de datos de DiffServ	425
39.	Relación entre los almacenamientos intermedios, las colas y el planificador	427
40.	Ejemplo de red L2TP	444
41.	Red que ejecuta NAT	470
42.	Red que ejecuta NAT	473
43.	Ejemplo de un Servidor DIAL dando soporte a marcación de entrada	487
44.	Adición de una interfaz de marcación de entrada	490
45.	Conceptos sobre el ámbito	513

46.	Network Station remota sin un Thin Server	579
47.	Network Station remota con un Thin Server	579
48.	Configuración de ejemplo de TSF	584

Tablas

1.	Funciones de código soportadas en el 2216 Modelo 400 y en Network Utility	xxxii
2.	Resumen de mandatos de configuración de la reserva de ancho de banda (disponible en el indicador BRS Config>)	27
3.	Mandatos de configuración de interfaz BRS disponibles en el indicador BRS [i #] Config> para interfaces Frame Relay	28
4.	Mandatos de gestión de clases de tráfico BRS	29
5.	Resumen de los mandatos de supervisión de la Reserva de ancho de banda	51
6.	Resumen de los mandatos de configuración del filtrado MAC	59
7.	Resumen de los submandatos de actualización	64
8.	Resumen de los mandatos de supervisión del filtrado MAC	68
9.	Resumen de los mandatos de configuración de Restauración de WAN	77
10.	Mandatos de supervisión de la Restauración de WAN	86
11.	Mandatos para establecer el alias del dispositivo de bucle de retorno (lo0) para Dispatcher	118
12.	Mandatos para suprimir rutas para diversos sistemas operativos	119
13.	Mandatos de configuración de Network Dispatcher	125
14.	Nombres de consejero y números de puerto	126
15.	Límites de configuración de los parámetros	132
16.	Mandatos de supervisión de Network Dispatcher	145
17.	Resumen de los mandatos de configuración de la Antememoria de Host On-Demand Client	160
18.	Resumen de mandatos de supervisión de la Antememoria de Host On-Demand Client	164
19.	Resumen de los mandatos de configuración de la Antememoria del servidor de la web	214
20.	Resumen de los mandatos de supervisión de la Antememoria del servidor de la web	222
21.	Mandatos de configuración del ES	230
22.	Mandato de supervisión del ES	232
23.	Mandatos de configuración de la compresión de datos PPP	243
24.	Mandatos de supervisión de la compresión de datos PPP	244
25.	Mandatos de configuración de la compresión de datos	247
26.	Mandatos de supervisión de la compresión de datos Frame Relay	247
27.	Definir los protocolos de seguridad PPP	253
28.	Definir los protocolos de seguridad de inicio de sesión	254
29.	Definir los protocolos de seguridad de túnel	255
30.	Mandatos de configuración de autenticación	259
31.	Submandatos de login	261
32.	Submandatos de password-rules	263
33.	Submandatos de PPP	265
34.	Submandatos de server	267
35.	Submandatos de Tunnel	271
36.	Mandatos de configuración de perfil de usuario	273
37.	Resumen de los mandatos de configuración de la Calidad de los servicios (QoS)	292
38.	Resumen de los mandatos de configuración de la Calidad de los servicios (QoS) de LE Client	292

39.	Resumen de los mandatos de configuración de la Calidad de los servicios (QoS) de LE Client	297
40.	Resumen de los mandatos de supervisión de la Calidad de los servicios (QoS)	300
41.	Resumen de los mandatos de supervisión de QoS de LE Client	301
42.	Consultas de fase 1 de IKE y decisiones devueltas	309
43.	Consultas de fase 2 de IKE y decisiones devueltas	310
44.	Mandatos de configuración de política	343
45.	Mandatos de configuración de LDAP	359
46.	Mandatos de supervisión de política	363
47.	Algoritmos configurados con diversas políticas de túnel	392
48.	Resumen de los mandatos de configuración de la Seguridad de IP	393
49.	Algoritmos configurados con diversas políticas de túnel	405
50.	Resumen de los mandatos de supervisión de IKE	411
51.	Resumen de los mandatos de supervisión de PKI	413
52.	Resumen de los mandatos de supervisión de la Seguridad de IP	417
53.	Mandatos de configuración de DiffServ	431
54.	Mandatos de supervisión de DiffServ	437
55.	Mandatos de configuración de la interfaz L2 Tunneling	453
56.	Mandatos de configuración de la característica L2 Tunneling	456
57.	Mandatos de supervisión de L2 Tunneling	461
58.	Mandatos de configuración de NAT	477
59.	Mandatos de supervisión de NAT	485
60.	Mandatos de configuración global de DIAL	495
61.	Mandatos de supervisión global de DIAL	503
62.	Resumen de los mandatos de configuración del servidor DHCP	539
63.	Resumen de los mandatos de supervisión del servidor DHCP	573
64.	Resumen de los mandatos de configuración del TSF	591
65.	Resumen de los mandatos de supervisión del TSF	601
66.	Mandatos de supervisión de VCRM	610

Avisos

Las referencias hechas en esta publicación a productos, programas o servicios de IBM no implican que IBM tenga la intención de comercializarlos en todos los países en los que realiza operaciones. 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. La evaluación y verificación del funcionamiento junto con otros productos, excepto los expresamente indicados por IBM, son responsabilidad del usuario.

IBM puede tener patentes o solicitudes de patentes pendientes que cubran temas tratados en este documento. La entrega de este documento no otorga ninguna licencia sobre estas patentes. Puede enviar por escrito consultas acerca de licencias a: IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785, Estados Unidos.

IBM proporciona el programa bajo licencia descrito en este documento y todo el material bajo licencia disponible para el mismo según los términos del Acuerdo con el cliente de IBM.

Este documento no está pensado para usos de producción y se proporciona tal cual sin garantías de ninguna clase, de modo que por el presente se rechazan todas las garantías, incluidas las de comercialización e idoneidad para un fin determinado.

Aviso para los usuarios de versiones en línea de este manual

Con respecto a las versiones en línea de este manual, está autorizado a:

- Copiar, modificar e imprimir la documentación contenida en el soporte, para utilizarla en la empresa, siempre y cuando reproduzca el aviso de copyright, todas las declaraciones de aviso y otras declaraciones necesarias en cada copia o copia parcial.
- Transferir la copia original de la documentación sin alteraciones cuando transfiera el producto de IBM relacionado (que pueden ser máquinas propiedad del usuario o programas, si los términos de la licencia del programa permiten una transferencia). Al mismo tiempo, debe destruir todas las otras copias de la documentación.

El usuario es responsable del pago de cualquier impuesto, incluidos los de propiedades personales, que derive de esta autorización.

NO HAY NINGUNA GARANTÍA, EXPLÍCITA NI IMPLÍCITA, INCLUIDAS LAS DE COMERCIALIZACIÓN E IDONEIDAD PARA UN FIN DETERMINADO.

Algunas jurisdicciones no permiten la exclusión de garantías implícitas, por lo que es posible que la exclusión anterior no afecte al usuario.

La renuncia a ajustarse a los términos descritos anteriormente dará término a esta autorización. Una vez que haya terminado, el usuario deberá destruir la documentación que pueda leer la máquina.

Marcas registradas

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

Advanced Peer-to-Peer Networking	IBM	PS/2
AIX	Micro Channel	RS/6000
AIXwindows	NetView	System/370
APPN	AS/400	Nways
VTAM	BookManager	ESCON

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

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

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

Prefacio

Este manual contiene la información que necesitará para utilizar la interfaz de usuario del direccionador para realizar la configuración y la operación de las características instaladas en su dispositivo Nways. Es posible que un dispositivo Nways específico no dé soporte a todas las características descritas en este manual. Si una característica es específica de un dispositivo, se le informará de ello mediante uno de los siguientes métodos:

- Una nota de aviso en el capítulo o la sección pertinente
- Una sección en el prefacio que contiene una lista de las características y los dispositivos que les dan soporte

Este manual da soporte al IBM 2216 y se refiere al mismo como el “direccionador” o un “dispositivo”. Los ejemplos incluidos en el manual representan la configuración de un IBM 2216, pero la salida que verá realmente puede ser diferente. Utilice los ejemplos como directrices de lo que podría ver mientras configura el dispositivo.

A quién va dirigido este manual

Este manual está destinado a las personas que instalan y gestionan redes informáticas. Aunque le será útil tener experiencia con el hardware y el software de las redes informáticas, no necesita tener experiencia de programación para utilizar el software de protocolos.

Para obtener información adicional: Pueden efectuarse cambios en la documentación después de que se impriman los manuales. Si está disponible información adicional o son necesarios cambios después de que se hayan impreso los manuales, encontrará los cambios en un archivo (denominado README) del disquete 1 del grupo de disquetes del programa de configuración. Podrá visualizar el archivo con un editor de texto ASCII.

Acerca del software

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

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

El código base viene instalado de fábrica en el 2216.

- El programa de configuración Programa de configuración para IBM Nways Multiprotocol Access Services (denominado así en este manual: *Programa de*

configuración) es una interfaz gráfica de usuario que permite configurar el dispositivo desde una estación de trabajo autónoma. El Programa de configuración incluye la función de comprobación de errores e información de ayuda en línea.

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

También puede obtener el Programa de configuración para IBM Nways Multiprotocol Access Services a partir de la página de presentación del soporte técnico de la red de IBM. Consulte el manual *Programa de configuración Guía del usuario para Nways Multiprotocol Access Services Products*, GC30-3830, para obtener la dirección de servidor y los directorios.

Convenios utilizados en este manual

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

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

```
reload
```

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

2. Las opciones de palabra clave para un parámetro van encerradas 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 encerrados entre corchetes inmediatamente después de la opción. Por ejemplo:

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

En este ejemplo, el medio 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 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*

Visión general de la biblioteca

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

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

Actualizaciones y correcciones de la información: Para mantenerse informado de los cambios técnicos, aclaraciones y arreglos implementados después de la impresión de los manuales, consulte las páginas de presentación del IBM 2216 en:

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

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

Planificación

GA27-4105 *IBM 2216 Introduction and Planning Guide*

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

Instalación

GA27-4106 *IBM 2216 Nways Multiaccess Connector Installation and Initial Configuration Guide*

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

GX27-3988 *2216 Nways Multiaccess Connector Hardware Configuration Quick Reference*

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

Diagnósticos y mantenimiento

SY27-0350 *2216 Nways Multiaccess Connector Service and Maintenance Manual*

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

Gestión de red y operaciones

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

SC10-3434 *Guía del usuario de software*

En este manual se explica cómo:

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

SC10-3429 *Utilización y configuración de las características*

SC10-3432 *Consulta de configuración y supervisión de protocolos Volumen 1*

SC10-3433 *Consulta de configuración y supervisión de protocolos Volumen 2*

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

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

SC30-3682 *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

GC10-3430 *Programa de configuración Guía del usuario para Nways Multiprotocol Access Services Products*

Este manual describe cómo utilizar el Programa de Configuración.

Seguridad

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

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

Marketing

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

Esta página web de IBM proporciona información sobre los productos a través de la World Wide Web.

Resumen de los cambios para la Biblioteca de software de IBM 2216

La lista siguiente se refiere a los cambios que se han efectuado en la versión 3.3 con respecto al software. Los cambios consisten en:

- **Nuevas funciones:**

- El Subsistema de codificación (ES)
- Los servicios del protocolo Dynamic Host Configuration Protocol (DHCP)
- La red privada virtual (VPN)
 - Los servicios de directorios: el soporte del protocolo Lightweight Directory Access Protocol (LDAP)
 - El soporte de ISAKMP/Oakley
 - Layer 2 Forwarding (L2F)
 - Point to Point Tunneling Protocol (PPTP)
 - Servicios diferenciados
- La fragmentación de paquetes de Frame Relay
- El reenvío de paquetes de Voz sobre Frame Relay

- **Funciones mejoradas:**

- Mejoras en IP
 - La política genérica de direccionamiento de IPv4
 - Los filtros de paquetes de IPv6, la reconfiguración dinámica y el soporte de los agentes de relay de DHCP
- Mejoras en SDLC
 - El sondeo de grupos primarios
 - La comunicación simultánea en dos direcciones
- Los parámetros de configuración de DLSw para permitir el control del número de mensajes sin sesión puestos en cola en el direccionador
- Las mejoras en el rendimiento de la función Thin Server
- Mejoras en TN3270
 - La antememoria de IBM eNetwork Host on-Demand Client
 - La definición de LU dinámica iniciada por sistema principal
 - Múltiples SA de PU sobre DLSw
- La mejora en la función de puente
 - El soporte de SR-TB de IPX
- El soporte de la reconfiguración dinámica de X.25
- Mejoras en IPX
 - Los ciclos de RIP configurables
 - Los SVC IPXWAN sobre Frame Relay
- La función de finalización de mandatos de la interfaz de línea de mandatos
- Mejoras en la antememoria del servidor de la web
 - El gestor de control de antememoria externa
 - Las mejoras en la escalabilidad y disponibilidad

- **Aclaraciones y correcciones**

Las adiciones y los cambios técnicos se indican mediante una línea vertical (|) situada a la izquierda del cambio.

Programa de utilidad de red

El Programa de utilidad de red es un producto que se compone de varios modelos del 2216. Proporciona varios subconjuntos de las funciones del 2216, tal como se muestra en Tabla 1.

Funciones de software soportadas por Network Utility

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

Tabla 1 (Página 1 de 3). Funciones de código soportadas en el 2216 Modelo 400 y en Network Utility

Función o protocolo	Disponible para el 2216 Modelo 400 Base	Disponible para la WSC del 2216 Modelo 400	Disponible para Network Utility Modelo TN1	Disponible para Network Utility Modelo TX1
TN3720E	sí ¹	—	sí ¹	—
Antememoria de IBM eNetwork Host on-Demand Client para TN3720E	sí ¹	—	sí ¹	—
Definición de LU dinámica iniciada por sistema principal para TN3720E	sí ¹	—	sí ¹	—
Múltiples SA de PU sobre DLSw para TN3720E	sí ¹	—	sí ¹	—
Network Dispatcher	sí	sí	sí	sí
Server Advisor (o Network Dispatcher Advisor) para TN3720E	sí	sí ²	sí	sí ²
Reserva de ancho de banda y puesta en cola según prioridad	sí	sí	sí	sí
Fragmentación de paquetes de Frame Relay	sí	sí	sí	sí
Reenvío de paquetes de Voz sobre Frame Relay	sí	sí	sí	sí
Filtración MAC	sí	sí	sí	sí
Restauración de WAN	sí	sí	—	—
Redireccionamiento de WAN	sí	sí	—	—

Tabla 1 (Página 2 de 3). Funciones de código soportadas en el 2216 Modelo 400 y en Network Utility

Función o protocolo	Disponible para el 2216 Modelo 400 Base	Disponible para la WSC del 2216 Modelo 400	Disponible para Network Utility Modelo TN1	Disponible para Network Utility Modelo TX1
Compresión de datos	sí	sí	sí	sí
Subsistema de codificación	sí	sí	sí	sí
Cifrado	sí	sí	sí	sí
Conmutación del enlace de datos (DLSw)	sí	—	sí	sí
Calidad de los servicios (QoS)	sí	sí	sí	sí
IPSec (Seguridad de IP)	sí	sí	sí	sí
Servicios diferenciados	sí	sí	sí	sí
L2TP	sí	sí	sí	sí
L2F	sí	sí	sí	sí
PPTP	sí	sí	—	—
Conversión de direcciones de red	sí	sí	sí	sí
AAA (Seguridad de la autenticación, autorización y contabilidad)	sí	sí	sí	sí
RSVP	sí	sí	sí	sí
Servicios de DHCP	sí	sí	sí	sí
Servicios de directorios: el soporte de LDAP	sí	sí	sí	sí
IPv6	sí	—	sí	sí
Thin Server	sí	—	—	—
Antememoria del servidor de la web	—	sí	—	—
Sondeo de grupos primarios para SDLC	sí	—	sí	sí
Comunicación simultánea en dos direcciones para SDLC	sí	—	sí	sí
IPX	sí	—	—	—
Appletalk	sí	—	—	—
DECnet IV	sí	—	—	—
OSI	sí	—	—	—
Banyan Vines	sí	—	—	—
DIAL	sí	sí	sí ³	sí ³
Funciones de APPN				
Branch Extender	sí	—	sí	sí
Peticionario de LU dependientes (DLuR)	sí	—	sí	sí

Tabla 1 (Página 3 de 3). Funciones de código soportadas en el 2216 Modelo 400 y en Network Utility

Función o protocolo	Disponible para el 2216 Modelo 400 Base	Disponible para la WSC del 2216 Modelo 400	Disponible para Network Utility Modelo TN1	Disponible para Network Utility Modelo TX1
Enterprise Extender	sí	—	sí	sí
Extended Border Node	sí	—	sí	sí
Direccionamiento de alto rendimiento (HPR)	sí	—	sí	sí
Nodo de red (NN)	sí	—	sí	sí

1. Ésta es una función cuyo precio va aparte
 2. En la comunicación con un servidor TN3270E de un producto de direccionamiento de IBM
 3. Sólo accesible si se utilizan las funciones de túnel. Las funciones de túnel incluyen L2TP, PPTP y L2F.

Cómo obtener ayuda

En los indicadores de mandatos, puede obtener ayuda en forma de listado de los mandatos disponibles del nivel actual. Para ello, escriba **?** (el mandato **help**) y luego pulse **Intro**. Utilice **?** para listar los mandatos disponibles que hay en el nivel actual. Normalmente, puede entrar el signo **?** después de un nombre de mandato específico si desea listar las opciones del mismo.

Cómo salir de un entorno de nivel inferior

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

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

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

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

Utilización de la reserva de ancho de banda y puesta en cola por prioridad

Este capítulo describe las características del Sistema de reserva de ancho de banda (BRS) y puesta en cola por prioridad que están disponibles para las interfaces Frame Relay y PPP. Incluye las secciones siguientes:

- “Sistema de reserva de ancho de banda”
- “Reserva de ancho de banda a través de Frame Relay” en la página 3
- “Sistema de colas de prioridad” en la página 6
- “BRS y filtrado” en la página 8
- “Configuraciones de ejemplo” en la página 13

Sistema de reserva de ancho de banda

El Sistema de reserva de ancho de banda (BRS) permite decidir cuáles son los paquetes que se deben eliminar cuando la demanda (tráfico) es mayor que la oferta (productividad) en una conexión de red. Cuando la utilización del ancho de banda alcance el 100%, BRS determinará cuáles son los elementos del tráfico que se eliminarán, según su configuración.

La reserva de ancho de banda "reserva" el ancho de banda de transmisión para unas clases de tráfico específicas. Cada clase tiene asignado un porcentaje mínimo del ancho de banda de la conexión. Vea la Figura 1 en la página 2 y la Figura 2 en la página 2.

En las interfaces PPP se definen las clases de tráfico (clases-t), y a cada clase de tráfico se le asigna un porcentaje del ancho de banda de la interfaz PPP. Hay al menos dos clases de tráfico:

1. Una clase LOCAL, a la que se asigna ancho de banda para los paquetes originados localmente por el direccionador (por ejemplo, paquetes IP RIP)
2. Una clase DEFAULT, a la que inicialmente se asigna todo el resto del tráfico.

Puede crear clases de tráfico adicionales y asignar protocolos, filtros y códigos a las colas de prioridad en una clase de tráfico. Vea la Figura 1 en la página 2.

En las interfaces Frame Relay se definen clases de circuito (clases-c) y a cada clase de circuito se le asigna un porcentaje del ancho de banda de la interfaz Frame Relay. Hay, al menos, una clase de circuito: la clase de circuito DEFAULT a la que se asignan inicialmente todos los circuitos. Puede crear clases de circuito adicionales y asignar circuitos a estas clases-c. En cada circuito Frame Relay, puede definir clases de tráfico (clases-t) y a cada clase de tráfico se le asigna un porcentaje del ancho de banda del circuito Frame Relay. El soporte a las clases de tráfico para los circuitos Frame Relay es análogo al soporte a las clases de tráfico para las interfaces PPP. Vea la Figura 2 en la página 2 para conocer las relaciones entre la clase de circuito Frame Relay y las clases de tráfico.

Utilización de BRS y puesta en cola por prioridad

Clase tráfico	Porcentaje de ancho banda interfaz	Cola prioridad	Tipo de tráfico
LOCAL	10%		
DEFAULT	40%	URGENT HIGH NORMAL LOW	(Protocolo, Código, Filtro) (Protocolo, Código, Filtro) Protocolo (Código, Filtro) (Protocolo, Código, Filtro)
CLASS A	xx%	URGENT HIGH NORMAL LOW	(Protocolo, Código, Filtro) (Protocolo, Código, Filtro) (Protocolo, Código, Filtro) (Protocolo, Código, Filtro)

Conexión PPP (BRS [i #])

Nota: Todos los protocolos se asignan inicialmente a la cola de prioridad NORMAL de la clase de tráfico DEFAULT. Puede asignar un protocolo, un filtro o un código a cualquier cola de prioridad en una clase de tráfico.

Figura 1. Relación entre la clase de tráfico BRS PPP y las colas de prioridad de las clases de tráfico

Clase circuito	Porcentaje ancho banda	(BRS [i #] [dpci #] Config>)	Número circuito	Filtro BRS	Especificación clase tráfico
DEFAULT	40%		16	habilitado	con valor por omisión *
			17	inhabilitado	sin filtro de tráfico
			18	habilitado	específico de circuito:
					LOCAL 10%
					DEFAULT 40%
					URGENT (protocolo, código, filtro) DE ** HIGH (protocolo, código, filtro) DE NORMAL protocolo (código, filtro) DE LOW (protocolo, código, filtro) DE
CLASS A	xx%		20		con valores por omisión *
			21		con valores por omisión *
.			.		
.			.		
.			.		
Otras definiciones de clase de circuito ...					
** Representa que los datos son elegibles para su borrado					
* Definiciones de clase de tráfico de circuito por omisión (BRS [i #] [Circuit Default] Config>)					
LOCAL	10%				
DEFAULT	40%				URGENT (protocolo, código, filtro) DE HIGH (protocolo, código, filtro) DE NORMAL protocolo (código, filtro) DE LOW (protocolo, código, filtro) DE
% de asignación de clase de circuito para clase de tráfico					

Conexión Frame Relay (BRS [i #] Config>)

Nota: Todos los protocolos se asignan inicialmente a la cola de prioridad NORMAL de la clase de tráfico DEFAULT. Puede asignar un protocolo, un filtro o un código a cualquier cola de prioridad en una clase de tráfico.

Figura 2. Relación entre la clase de circuito BRS Frame Relay y las clases de tráfico

Estos porcentajes reservados son una *porción* mínima del ancho de banda destinado a la conexión de red. Si una red funciona con plena capacidad, sólo pueden

transmitirse mensajes en cualquier clase hasta que utilicen el ancho de banda configurado que está asignado a la clase. En este caso, se retienen las transmisiones adicionales hasta que se hayan satisfecho otras transmisiones de ancho de banda. En caso de una vía de acceso de tráfico leve, una corriente de paquetes puede utilizar un ancho de banda que sobrepase el mínimo permitido hasta un 100% si no hay otro tipo de tráfico.

La reserva de ancho de banda es, en realidad, una medida de *precaución*. En general, un dispositivo no debe intentar utilizar más del 100% de su velocidad de línea. Si lo hace, probablemente se necesita una línea más rápida. Sin embargo, el carácter del tráfico, con repentinas “avalanchas”, puede hacer que la velocidad de transmisión solicitada sobrepase el 100% durante breves períodos de tiempo. En estos casos se habilita la reserva de ancho de banda y se asegura la transmisión del tráfico de prioridad más elevada (es decir, no se elimina).

La reserva de ancho de banda se ejecuta en los siguientes tipos de conexión:

- Frame Relay (interfaz de línea serie o circuito de marcación)
- PPP (interfaz de línea serie o circuito de marcación)

Reserva de ancho de banda a través de Frame Relay

La reserva de ancho de banda permite reservar ancho de banda a dos niveles:

- A nivel de interfaz, puede asignar un porcentaje del ancho de banda de la interfaz a las clases de circuito (*clases-c*). Cada clase de circuito contiene uno o más circuitos.
- A nivel de circuito, puede definir clases de tráfico (*clases-t*) y asignar un porcentaje del ancho de banda del circuito. (Una clase de tráfico creada por el mandato **create-super-class** no está asociada a ningún ancho de banda, sino que siempre tiene prioridad sobre todas las demás clases-t definidas para el circuito.)

Cuando BRS recibe un paquete de Frame Relay, las clases-c y las clases-t configuradas se utilizan para determinar cuándo se transmitirá ese paquete. BRS pone el paquete en cola según estos criterios: clase-c, circuito, clase-t y prioridad dentro de la clase-t. La clase-c a la que se ha asignado el circuito se pone en una cola de clases-c y la cola de clases-c se clasifica de acuerdo a un algoritmo de cola ponderado. En una clase-c, se da servicio de forma rotatoria a los circuitos que contienen paquetes que deben transmitirse. Las clases-t que hay en cada clase-c también se clasifican según un algoritmo de cola ponderado. En la clase-t, los paquetes se ponen en cola, además, según su prioridad (urgente, alta, normal o baja).

Un paquete se elimina de la cola y se transmite cuando cumple todos los criterios siguientes:

1. Es el paquete siguiente de la clase-c siguiente
2. Es el paquete siguiente del circuito siguiente de la clase-c
3. Es uno de los paquetes de la clase-t siguiente de esa clase-c
4. Es el paquete siguiente del grupo de prioridad siguiente de esa clase-t

Cuando se habilita la interfaz y uno o más circuitos para BRS, y no se configura ninguna clase-c o clase-t, todos los circuitos se asignan a una clase-c denominada *default* (por omisión). Con esta configuración, sólo existirá la clase-c por omisión

Utilización de BRS y puesta en cola por prioridad

en la cola de clases-c y cada circuito de la clase-c con paquetes que deben transmitirse se gestionará por orden rotatorio. Si desea que BRS lo haga, deje todos los circuitos en la clase-c por omisión y no cree ninguna otra clase de circuito.

Los circuitos huérfanos y los circuitos carentes de BRS habilitado explícitamente, utilizan este entorno de colas BRS por omisión en todas las estaciones. BRS los asigna a la clase-c por omisión (default).

Para configurar BRS, debe seguir esta secuencia:

1. Habilite BRS en la interfaz.
2. Habilite BRS en los circuitos y añada las clases-c.
3. Asigne los circuitos a las clases-c.
4. Si lo desea, defina clases-t para cada una de las clases-c.

Puede utilizar varios mandatos de supervisión de reserva de ancho de banda para visualizar contadores de reserva para las clases de circuito de una interfaz determinada:

- clear-circuit-class
- counters-circuit-class
- last-circuit-class

Consulte “Configuración y supervisión de reserva de ancho de banda” en la página 25 para obtener más información acerca de la supervisión de BRS.

La interfaz es la que aparece en el indicador para los mandatos de supervisión de ancho de banda. Por ejemplo, BRS [i 5] es el indicador correspondiente a la interfaz 5.

Soporte de colas

Con la reserva de ancho de banda a través de Frame Relay, cada circuito puede poner tramas en cola mientras está en estado congestionado, incluso para las interfaces y los circuitos que no estén habilitados para la reserva de ancho de banda.

Elegibilidad de eliminación

La red Frame Relay puede eliminar los datos transmitidos que sobrepasen la CIR en un PVC. El direccionador puede definir el bit DE para indicar que una parte del tráfico debe considerarse como elegible para su eliminación. Si es adecuado, la red Frame Relay eliminará las tramas marcadas como elegibles para eliminación, lo que permite que las tramas no marcadas como elegibles para eliminación puedan atravesar la red. Al asignar un protocolo, un filtro o un código a una clase de tráfico, puede especificar si el tráfico de protocolos, filtros o códigos es elegible para eliminación. Consulte “Assign” en la página 33 para obtener más información sobre cómo configurar el tráfico como elegible para eliminación. El tráfico de voz (identificada por el protocolo VOFR) debe configurarse siempre como **no** elegible para eliminación.

Definiciones de circuito por omisión para la gestión de clases de tráfico

Las interfaces Frame Relay pueden tener definidos numerosos circuitos. En lugar de tener que configurar por completo las definiciones de clases de tráfico para cada circuito, BRS permite definir por omisión un conjunto de clases de tráfico y asignaciones de protocolos, filtros y códigos, denominado definiciones de circuito por omisión, que cualquier circuito en la interfaz pueda utilizar. Cuando se habilita BRS inicialmente en un circuito, éste se inicializa para utilizar definiciones de circuito por omisión. Si un circuito no puede utilizar las definiciones de circuito por omisión para la gestión de clases de tráfico, puede crear definiciones específicas del circuito mediante los mandatos **add-class**, **change-class**, **assign**, **deassign**, **tag** y **untag**.

Si un circuito utiliza definiciones específicas de circuito y quiere usar en su lugar las definiciones de circuito por omisión, puede utilizar el mandato **use-circuit-defaults** en el indicador BRS del circuito.

Las definiciones de circuito por omisión para la gestión de clases de tráfico se definen mediante **set-circuit-defaults** en el indicador de la interfaz BRS Frame Relay. Este mandato le permite acceder a un indicador de valores por omisión de circuito BRS en el que puede añadir, cambiar y suprimir clases de tráfico, asignar y desasignar protocolos, filtros y códigos, y crear códigos BRS. Los cambios en las definiciones de circuito por omisión para las clases de tráfico dan como resultado unas actualizaciones dinámicas a la gestión de clases de tráfico para todos los circuitos utilizando las definiciones de circuitos por omisión.

Configuración de BRS para la voz a través de Frame Relay

Las tramas de voz pueden transportarse a través de circuitos dedicados. En esta situación, habilite BRS en la interfaz y en los circuitos y acepte los valores por omisión en los circuitos asociados con la voz. Tal vez desee crear varias clases-c y asignar los circuitos dedicados a voz a una clase-c que esté asociada a un porcentaje grande de ancho de banda, así como asignar los circuitos asociados a datos a una clase de circuito asociada a un porcentaje de ancho de banda más pequeño.

Si el tráfico de voz y de otros tipos se transporta a través de los mismos circuitos, habilite BRS en la interfaz y en los circuitos. Si desea que se dé servicio a todos los circuitos de forma rotatoria sin favorecer a uno o más circuitos, puede optar por no crear clases-c adicionales aparte de la clase-c por omisión. Entonces, para cada circuito a través del cual se transporten voz y datos, se sugiere que cree una clase-t con el mandato **create-super-class** y asigne el tráfico VOFR a esta clase. Cree también clases-t adicionales como considere necesario y asigne otros tipos de tráfico a estas clases-t. Esta configuración contribuirá a que el tráfico de voz tenga prioridad sobre el resto del tráfico y, si la fragmentación está habilitada, que las tramas de voz no segmentadas puedan intercalarse entre segmentos de datos fragmentados. Se recomienda que habilite la fragmentación en la interfaz Frame Relay si va a enviar voz y datos a través de la misma interfaz. La fragmentación causará que haya tramas más pequeñas y, por consiguiente, un retardo menor entre tramas de voz consecutivas.

Consulte el mandato **enable fragmentation** en el capítulo “Configuring and Monitoring Frame Relay Interfaces” del manual *Nways Multiprotocol Access Services Guía del usuario de software* para obtener más información acerca de la habilitación de la fragmentación.

Sistema de colas de prioridad

La reserva de ancho de banda asigna porcentajes del ancho de banda de conexión total para *clases* de tráfico o *clases-t* específicas, definidas por el usuario. Excepto para una clase-t creada por el mandato **create-super-classpubs**, que tiene prioridad sobre todas las demás clases-t, las clases-t BRS están asociadas a un porcentaje de ancho de banda. Los protocolos y datos de filtro pueden asignarse a las clases-t y a colas de prioridad específicas en una clase-t. Con el sistema de colas de prioridad, puede asignarse un protocolo o un filtro a una cola específica en una clase de tráfico con valores: una clase-t BRS es un grupo de paquetes identificados con el mismo nombre; por ejemplo, una clase denominada “ipx” designa todos los paquetes IPX.

Con el sistema de colas de prioridad, a cada clase-t de ancho de banda se le puede asignar uno de los valores de nivel de prioridad siguientes:

- Urgent (urgente)
- High (alto)
- Normal (valor por omisión)
- Low (bajo)

para las clases de tráfico o clases-t específicas definidas por el usuario.

Además, puede definir el número de paquetes que aguardan en la cola para cada nivel de prioridad en cada clase-t de ancho de banda. El mandato **queue-length** BRS define el número máximo de almacenamientos intermedios de salida que pueden ponerse en cada cola de prioridad BRS, así como el número máximo de almacenamientos intermedios de salida que pueden ponerse en cada cola de prioridad BRS para el momento en que los almacenamientos intermedios de entrada de direccionador sean escasos. Puede configurar las longitudes de las colas de prioridad para PPP y para Frame Relay.

Atención: Si define unos valores demasiado elevados para la longitud de las colas, puede perjudicar gravemente al rendimiento del direccionador.

Para BRS, puede definir longitudes de las colas de prioridad para las conexiones WAN de PPP y Frame Relay. Consulte “Queue-length” en la página 47 para ver una descripción del mandato **queue-length**.

Los valores de prioridad de una clase-t de ancho de banda no tienen efecto sobre otras clases de anchos de banda. Ninguna clase de ancho de banda tiene prioridad sobre las demás.

Colas de prioridad sin reserva de ancho de banda

Cuando el sistema de colas de prioridad se configura sin realizar la reserva de ancho de banda, en primer lugar se suministra el tráfico de mayor prioridad. En los casos de tráfico pesado de alta prioridad, pueden desdeñarse los niveles de prioridad inferior. No obstante, al combinar el sistema de colas de prioridad con la reserva de ancho de banda, la transmisión de paquetes puede asignarse a todos los tipos de tráfico.

Configuración de clases de tráfico

Cree una clase de tráfico mediante el mandato **add-class** y, a continuación, asigne tipos de tráfico a la clase mediante el mandato **assign**. El tráfico se asigna a una clase de tráfico según su *tipo de protocolo* o según un filtro que identifica mejor un tipo específico de *tráfico de protocolos* (por ejemplo, paquetes IP SNMP).

Los tipos de protocolo soportados son:

- IP
- ARP
- DNA
- VINES
- IPX
- OSI
- VOFR
- AP2
- ASRT
- SNA/APPN-ISR
- APPN-HPR
- HPR/IP

Filtros BRS

Mediante la reserva de ancho de banda, puede tratar el tráfico de protocolos específico de manera distinta del resto del tráfico que utiliza el mismo tipo de protocolo. Por ejemplo, puede asignar el tráfico IP SNMP a una clase de tráfico y una prioridad diferentes de otros tipos de tráfico IP. En este ejemplo, SNMP es un filtro BRS porque *filtra* (es decir, identifica de forma exclusiva) el tráfico de protocolos específico. La reserva de ancho de banda puede filtrar el tráfico de protocolos IP, ASRT (puente) y APPN-HPR. Están soportados los siguientes filtros:

- Túnel IP
- Túnel SDLC a través de IP (SDLC Relay)
- Túnel BSC a través de IP (BSC Relay)
- Rlogin
- Telnet
- SNA/APPN-ISR
- APPN-HPR
- SNMP
- IP Multicast
- DLSw
- Filtro MAC
- NetBIOS
- Network-HPR
- HPR alto
- HPR medio
- HPR bajo
- XTP
- Números de puerto o zócalos TCP/UDP
- Byte TOS
- Bit de precedencia

BRS y filtrado

En las secciones siguientes se describe cómo utilizar BRS con diversos tipos de filtrado.

Filtrado y códigos de direcciones MAC

El filtrado de Direcciones MAC se gestiona mediante un esfuerzo conjunto de la reserva de ancho de banda y el filtrado MAC (MCF) mediante unos *códigos*. Por ejemplo, un usuario con reserva de ancho de banda puede establecer categorías de tráfico de puente asignándole un código.

El proceso de codificación se realiza creando un filtro en la consola de configuración de filtrado MAC y, después, asignándole un número de código. Este número de código se utiliza para configurar una clase de tráfico para todos los paquetes asociados a este código. Los valores de los códigos deben estar en el rango de 1 a 64. Consulte “Utilización del filtrado MAC” en la página 55 para obtener información adicional acerca del filtrado MAC.

Nota: Los códigos *sólo* pueden aplicarse a los paquetes con puente. En una conexión PPP o Frame Relay, puede asignarse un máximo de cinco filtros MAC codificados como filtros de reserva de ancho de banda y se designan como TAG1 a TAG5. Primero se busca TAG1, después TAG2, y así sucesivamente hasta TAG5. Un código de filtro MAC puede consistir en cualquier número de Direcciones MAC definidas en MCF.

Una vez que haya creado un filtro codificado en el proceso de configuración de filtrado MAC, puede utilizar el mandato de configuración tag de BRS para asignar un nombre de código BRS (TAG1, TAG2, TAG3, TAG4 o TAG5) al número de código de filtro MAC. A continuación, utilice el nombre de código BRS en el mandato assign BRS para asignar el filtro MAC correspondiente a una clase de tráfico y prioridad de ancho de banda.

Los códigos también pueden referirse a “grupos”, como en el ejemplo del Túnel IP. Los puntos finales de Túnel IP pueden pertenecer a cualquier cantidad de grupos. Los paquetes se asignan a un grupo determinado mediante la característica de codificación del filtrado de Dirección MAC. Para obtener información adicional acerca del filtrado MAC, consulte “Utilización del filtrado MAC” en la página 55 y “Configuración y supervisión del filtrado MAC” en la página 59.

Para aplicar la reserva de ancho de banda y la prioridad de colas a los paquetes codificados:

1. Utilice los mandatos de configuración de filtrado MAC en el indicador `filter config>` para configurar códigos para los paquetes que pasen por el puente. Consulte “Utilización del filtrado MAC” en la página 55 para obtener más información.
2. Utilice el mandato **tag** de reserva de ancho de banda para establecer una referencia en un código para la reserva de ancho de banda.
3. Con el mandato **assign** de reserva de ancho de banda, asignará el código BRS a una clase-t. El mandato **assign** le solicitará también una prioridad de colas en esa clase-t BRS.

Filtrado de números de puerto TCP/UDP

Puede asignar paquetes TCP/IP de un rango de puertos TCP o UDP a una clase-t BRS y prioridad basadas en el número de puerto UDP o TCP y, opcionalmente, en un zócalo. Puede especificar un máximo de 5 filtros de número de puerto UDP/TCP, donde los filtros especifican un número de puerto TCP o UDP individual, un rango de números de puerto TCP o UDP, o un identificador de zócalo (una combinación de número de puerto y dirección IP). A continuación, puede asignar ese filtro a una clase de tráfico BRS y una prioridad dentro de esa clase.

Si el filtrado de puertos UDP/TCP está habilitado, BRS consulta cada paquete TCP o UDP y comprueba si el número de puerto de destino o de origen coincide con uno de los números de puerto que ha especificado para el filtrado. Además, si define una dirección IP como parte del filtro UDP/TCP BRS y una dirección de destino o de origen coincide con la dirección de filtro que se ha definido, BRS asignará el paquete a la clase de tráfico y la prioridad correspondientes a ese filtro de número de puerto.

Por ejemplo, puede configurar un filtro de número de puerto UDP para los números de puerto UDP en el rango de 25 a 29 y asignar el filtro a la clase de tráfico 'A' con la prioridad 'normal'. BRS pone en cola cualquier número de paquetes UDP con un número de puerto de origen o destino de 25 a 29 en la cola de prioridad normal para la clase de tráfico 'A'.

También puede configurar un filtro de número de puerto TCP para el número de puerto TCP 50 para la dirección IP 5.5.5.25, y asignar el filtro a la clase de tráfico 'B' con la prioridad 'urgent'. BRS pone en cola cualquier número de paquetes TCP cuyo número de puerto de origen o destino de 50 y cuya dirección IP de destino o de origen sea 5.5.5.25 en la cola de prioridad urgente para la clase de tráfico 'B'.

Filtrado de bits TOS IPv4

Puede crear filtros que distingan entre tipos distintos de tráfico IP, basándose en los valores de los bits TOS (Tipo de servicio). Estos filtros TOS pueden utilizarse para asignar el tráfico IPv4, que tiene valores particulares de los bits TOS, para una clase y una prioridad diferentes que otros tipos de tráfico IP. Cada filtro permite el tráfico IPv4 cuyo valor de byte TOS coincida con la definición de un filtro TOS configurado que se debe asignar a una clase de tráfico y una prioridad exclusivas. La configuración de un filtro TOS incluye una especificación de valor de máscara para definir cuáles son los bits, dentro del byte TOS, que deben coincidir, así como la especificación de los valores de rango superior e inferior para los bits que estén dentro de la máscara. El mecanismo de filtrado se basa exclusivamente en valores TOS IPv4; por consiguiente, no se basa en la identificación de la información del tipo de protocolo IPv4 o número de puerto, como la mayoría de los demás filtros IP.

Este filtro tiene una aplicación más ampliable que el filtro de precedencia IPv4 BRS, que afecta únicamente a los 3 bits de orden superior del byte TOS. Cuando se combina con el soporte de control de acceso IP para definir bits TOS, el soporte de filtro de bit TOS BRS permite realizar el filtrado del tráfico que se envía a través de un túnel seguro, que está fragmentado, o que no puede identificarse mediante el soporte de filtros de número de puerto UDP y TCP BRS. Además, el soporte de control de acceso IP permite definir los bits TOS con un valor definido por el usuario, en vez de tener que utilizar los valores de bit de precedencia de código de hardware para APPN y DLSw que están asociados al filtrado de bits de

Utilización de BRS y puesta en cola por prioridad

precedencia IPv4 BRS. Por consiguiente, se recomienda que utilice el control de acceso IP y el soporte de filtros TOS BRS en lugar del filtrado de bits de precedencia IPv4 BRS.

Como se indica en “Orden de precedencia del filtrado” en la página 12, las coincidencias de los filtros TOS se comprueban antes que los filtros de bits de precedencia IPv4 y otros filtros específicos de IP. Comprueba que las coincidencias de los filtros TOS1 a TOS5 se realicen de forma secuencial, empezando por el filtro TOS1. Puede definirse un máximo de 5 filtros TOS.

Importante: Tenga en cuenta que un paquete con un valor de TOS determinado se gestiona según la primera definición de filtro TOS con que coincide el valor. Procure configurar los filtros de tal manera que sea un byte TOS determinado sea filtrado por el filtro previsto, no accidentalmente por un filtro de número inferior. Consulte “Using IP” en el manual *Utilización y configuración de las características* para obtener más información.

Utilización del proceso de bits de precedencia de IP Versión 4 para el tráfico SNA en túneles seguros IP y fragmentos secundarios

Normalmente, BRS diferencia el tráfico TCP y UDP IP, según sus números de puerto. No obstante, BRS no puede identificar los puertos después de que el tráfico se haya encapsulado dos veces, como el tráfico IP transportado a través de un túnel seguro IP o en un fragmento UDP o TCP secundario. El proceso de bits de precedencia IP versión 4 se ha añadido a BRS para permitirle filtrar los paquetes de túnel seguro IP o los paquetes de fragmentos secundarios TCP y UDP.

Nota: Se recomienda que utilice el filtrado de bits TOS IPv4 BRS, en lugar del proceso de bits de precedencia IPv4. Consulte “Filtrado de bits TOS IPv4” en la página 9 para obtener más detalles.

Cuando el tráfico APPN/HPR se direcciona a través de IP, cada prioridad de transmisión de APPN-HPR (red, alta, media o baja) se correlaciona con un valor determinado de los tres bits de precedencia IP versión 4.

- La prioridad de transmisión de red HPR se correlaciona con el valor de precedencia IPv4 '110'b.
- La prioridad de transmisión alta HPR se correlaciona con el valor de precedencia IPv4 '100'b.
- La prioridad de transmisión media HPR se correlaciona con el valor de precedencia IPv4 '010'b.
- La prioridad de transmisión baja HPR se correlaciona con el valor de precedencia IPv4 '001'b.

Cuando el filtrado de precedencia IPv4 está habilitado para BRS y los bits de precedencia en un paquete IP coinciden con uno de los valores utilizados para el tráfico APPN/HPR, el paquete se pone en la cola de prioridad de la clase-t BRS a la que se asigna la prioridad de transmisión HPR correspondiente. Por ejemplo, si un paquete IP tiene el valor de precedencia '110'b y el filtro de red HPR BRS se asigna a la clase-t A y el nivel de prioridad normal, el paquete se pone en la cola de prioridad normal de la clase-t A. Si un filtro de prioridad de transmisión HPR BRS no está configurado, pero el filtro APPN-HPR sí lo está, el paquete se pone en la cola de prioridad y en la clase-t a la que se asigna el filtro APPN-HPR.

Estas tres clases de tráfico se correlacionan con el valor de precedencia IPv4 '011'b:

- El tráfico XID APPN/HPR que se envía cuando APPN/HPR se direcciona a través de IP
- Tráfico DLSw
- Tráfico TN3270

Dado que varios tipos de tráfico se correlacionan con un valor, BRS no puede distinguir entre ellos cuando está habilitado para filtrar según los bits de precedencia IPv4. Por consiguiente, cuando BRS encuentra un paquete IP con un valor de precedencia '011'b, evalúa los filtros BRS en el siguiente orden para determinar si el filtro está habilitado o no. Cuando encuentra un filtro BRS que está configurado, el paquete se pone en la cola de prioridad y en la clase-t a la que está asignado el filtro BRS:

- SNA/APPN-ISR (utilizado para intercambios XID APPN/HPR)
- DLSw
- Telnet

Si un paquete tiene uno de los valores de precedencia que BRS filtra, pero no se ha configurado ninguno de los tipos de filtro BRS aplicables, el paquete se pone en la cola de prioridad y en la clase-t BRS a la que está asignado el protocolo IP.

Cuando un cliente envía tráfico TN3270 a 2216 a través de una red de área amplia en la que BRS está habilitado, BRS no puede dar prioridad al tráfico del cliente, a menos que el cliente defina los bits de precedencia como '011'b.

Debe configurar la gestión de bits de precedencia IPv4 en varios lugares:

1. En BRS, configure si BRS debe filtrar o no, basándose en los bits de precedencia IPv4. Sólo realiza este tipo de filtro para los paquetes de túnel seguro IP o paquetes de fragmentos secundarios TCP y UDP.
2. Al configurar DLSw, HPR a través de IP y TN3270, especifique si 2216 debe definir los bits de precedencia IPv4 para los paquetes que origina para cada uno de estos tipos de protocolo.

Realice estos tres pasos para utilizar el filtrado de bits de precedencia IPv4:

1. Active el filtrado de precedencia IPv4 en BRS.
2. Configure clases-t BRS y asigne protocolos y filtros para varias categorías de tráfico SNA, como lo haría con el tráfico SNA que no se transporte en un túnel seguro IP o no se fragmente.
3. Habilite el valor de los bits de precedencia IPv4 al configurar los protocolos de DLSw, HPR a través de IP y TN3270.
4. Configure IPsec para crear un túnel seguro a través del cual fluya el tráfico DLSw, HPR a través de IP y TN3270.

Filtrado SNA y APPN para el tráfico con puente

El filtro SNA/APPN-ISR permite asignar el tráfico SNA y APPN-ISR para el que se establece un puente a una clase de tráfico BRS. El tráfico SNA y APPN-ISR se identifica como cualquier puente con un SAP de destino o de origen 0x04, 0x08 ó 0x0C, y cuyo campo de control LLC (802.2) indica que no es una trama de información no numerada (UI).

Utilización de BRS y puesta en cola por prioridad

Nota: Los paquetes BAN de Frame Relay se encuentran en esta categoría.

Los filtros APPN-HPR permiten asignar el tráfico HPR para el que se establece un puente a una clase-t BRS. El tráfico HPR se identifica como cualquier paquete de puente con un SAP de destino o de origen X'04', X'08', X'0C' o X'C8' y cuyo campo de control LLC (802.2) indica que es una trama de información no numerada (UI).

Los filtros de HPR de Red, HPR Alto, HPR Medio y HPR Bajo permiten que continúe el filtrado del tráfico del puente según la prioridad de transmisión HPR. Por ejemplo, si desea asignar el tráfico HPR que utiliza la prioridad de transmisión de red a una clase-t y una prioridad, y todo el resto del tráfico de puente HPR a una clase-t o una prioridad diferentes, debería asignar el filtro HPR de Red a la clase-t y la prioridad adecuadas y utilizar el filtro APPN-HPR para asignar el resto del tráfico HPR a una clase-t o prioridad diferentes.

El tráfico APPN-HPR que se direcciona a través de IP se filtra mediante el número de puerto UDP asignado para las prioridades de transmisión HPR de red, alta, media y baja. Se utiliza un número de puerto UDP adicional para los intercambios de XID. Se pueden configurar todos los números de puerto UDP que se utilizan para dar soporte a APPN-HPR a través de IP.

Si APPN no está habilitado en un direccionador intermedio en la red IP, puede configurar números de puerto UDP para HPR a través de IP desde el indicador de mandatos BRS `Config`. Si APPN está habilitado en el dispositivo, BRS utilizará los valores configurados en el indicador de mandatos APPN `Config`.

Otros filtros le pueden ayudar a asignar el tráfico. Por ejemplo, el filtro DLSw le permite asignar el tráfico SNA-DLSw que se envía a través de una conexión TCP a una clase-t BRS.

Para los filtros SNA/APPN-ISR y APPN-HPR, si desea comprobar los SAP distintos de los indicados anteriormente, cree un filtro de ventana deslizante mediante el filtrado MAC y defina un código para ese filtro. A continuación, asigne el filtro MAC codificado a una clase-t BRS.

Orden de precedencia del filtrado

Es posible que un paquete coincida con más de un tipo de filtro BRS. Por ejemplo, un paquete de puente con túnel IP que contenga datos SNA podría coincidir con el filtro de túnel IP y el filtro SNA/APPN-ISR. El orden en que se evalúan los filtros para determinar si un paquete coincide o no con un tipo de filtro BRS es el siguiente:

1. Filtros TOS (IP)
2. Gestión de precedencia IPv4
3. Coincidencia de códigos de filtro MAC para paquetes de puente (IP/ASRT)
4. NetBIOS para puente (IP/ASRT)
5. SNA/APPN-ISR para puente (IP/ASRT)
6. HPR de Red (IP/ASRT/APPN-HPR)
7. HPR Alto (IP/ASRT/APPN-HPR)
8. HPR Medio (IP/ASRT/APPN-HPR)
9. HPR Bajo (IP/ASRT/APPN-HPR)
10. APPN-HPR (IP/ASRT)
11. Filtros de número de puerto UDP/TCP (IP)

12. Túnel IP (IP)
13. SDLC/BSC Relay (IP)
14. DLSw (IP)
15. Multidifusión (IP)
16. SNMP (IP)
17. Rlogin (IP)
18. Telnet (IP)
19. XTP (IP)

Nota: Los protocolos a los que es aplicable el filtro aparecen entre paréntesis.

Configuraciones de ejemplo

Utilización de definiciones de circuito por omisión para la gestión de clases de tráfico de circuitos Frame Relay

Notas:

- 1** Configurar la característica BRS.
- 2** Habilitar BRS en la interfaz 1.
- 3** Habilitar BRS en los circuitos 16, 17, 18. Se utilizan definiciones de circuito por omisión para la gestión de clases de tráfico para estos circuitos.
- 4** Acceder al menú set-circuit-defaults para establecer definiciones de circuito por omisión para la gestión de clases de tráfico.
- 5** Añadir clases de tráfico y asignar protocolos y filtros a las clases de tráfico.
- 6** Listar y mostrar las definiciones de BRS para el circuito 16. Dado que el circuito 16 utiliza definiciones de circuito por omisión, se visualizan las clases de tráfico y las asignaciones de protocolos y filtros definidas por las definiciones de circuito por omisión.
- 7** Cambiar el circuito 17 para que, en vez de utilizar definiciones de circuito por omisión, utilice definiciones específicas de circuito para la gestión de clases de tráfico creando una clase exclusiva, CIRC171. A esta clase se le pueden asignar protocolos, filtros o códigos.
- 8** Cambiar las definiciones de circuito por omisión de tal manera que cada una de las clases de tráfico DEF1 y DEF2 reserven un 10% del ancho de banda y, a continuación, muestren que estos cambios son adoptados por el circuito 16 pero no por el circuito 17, dado que éste utiliza ahora definiciones específicas del circuito.
- 9** Alterar el circuito 17 para utilizar las definiciones de circuito por omisión para la gestión de clases de tráfico en lugar de las definiciones específicas de circuito.

Utilización de BRS y puesta en cola por prioridad

```
t 6
Gateway user configuration
Config>feature brs 1
Bandwidth Reservation User Configuration
BRS Config>interface 1 2
BRS [i 1]Config>enable
Please reload router for this command to take effect.
BRS [i 1] Config>circuit 16 3
BRS [i 1][dlci 16] Config>enable
Defaults are in effect for this circuit.
Please reload router for this command to take effect.
BRS [i 1][dlci 16] Config>exit
BRS [i 1]Config>circuit 17
BRS [i 1][dlci 17] Config>enable
Defaults are in effect for this circuit.
Please reload router for this command to take effect.
BRS [i 1][dlci 17] Config>exit
BRS [i 1]Config>circuit 18
BRS [i 1][dlci 18] Config>enable
Defaults are in effect for this circuit.
Please reload router for this command to take effect.
BRS [i 1][dlci 18] Config>
*reload
Are you sure you want to reload the gateway? (Yes or [No]): yes
```

```
*t 6
Gateway user configuration
Config>feature brs
Bandwidth Reservation User Configuration
BRS Config>interface 1
BRS[i 1] Config>list

BANDWIDTH RESERVATION listing from SRAM
bandwidth reservation is enabled
interface number 1
maximum queue length 10, minimum queue length 3
total bandwidth allocated 10%
total circuit classes defined (counting one default) 1

class DEFAULT has 10% bandwidth allocated
the following circuits are assigned:
    16 using defaults.
    17 using defaults.
    18 using defaults.

default class is DEFAULT
```

```

BRS [i 1] Config>?
ENABLE
DISABLE
SET-CIRCUIT-DEFAULTS
CIRCUIT
ADD-CIRCUIT-CLASS
DEL-CIRCUIT-CLASS
CHANGE-CIRCUIT-CLASS
DEFAULT-CIRCUIT-CLASS
ASSIGN-CIRCUIT
DEASSIGN-CIRCUIT
QUEUE-LENGTH
LIST
SHOW
CLEAR-BLOCK
EXIT
BRS [i 1] Config>set-circuit-defaults 4
BRS [i 1] [circuit defaults] Config>?
ADD-CLASS
DEL-CLASS
CHANGE-CLASS
DEFAULT-CLASS
TAG
UNTAG
ASSIGN
DEASSIGN
LIST
EXIT
BRS [i 1] [circuit defaults] Config>add 5
Class name [DEFAULT]?DEF1
Percent bandwidth to reserve [10]? 5
BRS [i 1] [circuit defaults] Config>add
Class name [DEFAULT]?DEF2
Percent bandwidth to reserve [10]?5
BRS [i 1] [circuit defaults] Config>assign ip
Class name [DEFAULT]?DEF1
Priority <URGENT/HIGH/NORMAL/LOW> [NORMAL]?
Frame Relay Discard Eligible <NO/YES> [NO]?
BRS [i 1] [circuit defaults] Config>assign asrt
Class name [DEFAULT]? DEF2
Priority <URGENT/HIGH/NORMAL/LOW> [NORMAL]?
Frame Relay Discard Eligible <NO/YES> [NO]?
BRS[i 1] [circuit defaults] Config>list

BANDWIDTH RESERVATION listing from SRAM
bandwidth reservation is enabled
interface number 1, default circuit
total bandwidth allocated 60%
total classes defined (counting one local and one default) 4

class LOCAL has 10% bandwidth allocated
  protocols and filters cannot be assigned to this class.

```

Utilización de BRS y puesta en cola por prioridad

```
class DEFAULT has 40% bandwidth allocated
  the following protocols and filters are assigned:
    protocol ARP with default priority is not discard eligible
    protocol DNA with default priority is not discard eligible
    protocol VINES with default priority is not discard eligible
    protocol IPX with default priority is not discard eligible
    protocol OSI with default priority is not discard eligible
    protocol VOFR with default priority is not discard eligible
    protocol AP2 with default priority is not discard eligible

class DEF1 has 5% bandwidth allocated
  the following protocols and filters are assigned:
    protocol IP with priority NORMAL is not discard eligible

class DEF2 has 5% bandwidth allocated
  the following protocols and filters are assigned:
    protocol ASRT with priority NORMAL is not discard eligible

assigned tags:

default class is DEFAULT with priority NORMAL

BRS [i 1] [circuit defaults] Config>exit
BRS [i 1] Config>circuit 16 6
BRS [i 1][dlci 161] Config>list

BANDWIDTH RESERVATION listing from SRAM
bandwidth reservation is enabled
interface number 1, circuit number 16 using defaults.
maximum queue length 10, minimum queue length 3
total bandwidth allocated 60%
total classes defined (counting one local and one default) 4

class LOCAL has 10% bandwidth allocated
  protocols and filters cannot be assigned to this class.

class DEFAULT has 40% bandwidth allocated
  the following protocols and filters are assigned:
    protocol ARP with default priority is not discard eligible
    protocol DNA with default priority is not discard eligible
    protocol VINES with default priority is not discard eligible
    protocol IPX with default priority is not discard eligible
    protocol OSI with default priority is not discard eligible
    protocol VOFR with default priority is not discard eligible
    protocol AP2 with default priority is not discard eligible

class DEF1 has 5% bandwidth allocated
  the following protocols and filters are assigned:
    protocol IP with priority NORMAL is not discard eligible

class DEF2 has 5% bandwidth allocated
  the following protocols and filters are assigned:
    protocol ASRT with priority NORMAL is not discard eligible

assigned tags:

default class is DEFAULT with priority NORMAL
```

Utilización de BRS y puesta en cola por prioridad

BRS [i 1] [d1ci 16] Config>**show**

BANDWIDTH RESERVATION currently in RAM
interface number 1, circuit number 16 using defaults.
maximum queue length 10, minimum queue length 3
4 current defined classes:
class LOCAL has 10% bandwidth allocated
class DEFAULT has 40% bandwidth allocated
class DEF1 has 5% bandwidth allocated
class DEF2 has 5% bandwidth allocated

protocol and filter assignments:

Protocol/Filter	Class	Priority	Discard Eligible
IP	DEF1	NORMAL	NO
ARP	DEFAULT	NORMAL	NO
DNA	DEFAULT	NORMAL	NO
VINES	DEFAULT	NORMAL	NO
IPX	DEFAULT	NORMAL	NO
OSI	DEFAULT	NORMAL	NO
VOFR	DEFAULT	NORMAL	NO
AP2	DEFAULT	NORMAL	NO
ASRT	DEF2	NORMAL	NO

BRS [i 1] [d1ci 16] Config>**exit**

Utilización de BRS y puesta en cola por prioridad

```
BRS [i 1] Config>circuit 17
BRS [i 1] [dlci 17] Config>list

BANDWIDTH RESERVATION listing from SRAM
bandwidth reservation is enabled
interface number 1, circuit number 17 using defaults.
maximum queue length 10, minimum queue length 3
total bandwidth allocated 60%
total classes defined (counting one local and one default) 4

class LOCAL has 10% bandwidth allocated
  protocols and filters cannot be assigned to this class.

class DEFAULT has 40% bandwidth allocated
  the following protocols and filters are assigned:
    protocol ARP with default priority is not discard eligible
    protocol DNA with default priority is not discard eligible
    protocol VINES with default priority is not discard eligible
    protocol IPX with default priority is not discard eligible
    protocol OSI with default priority is not discard eligible
    protocol VOFR with default priority is not discard eligible
    protocol AP2 with default priority is not discard eligible

class DEF1 has 5% bandwidth allocated
  the following protocols and filters are assigned:
    protocol IP with priority NORMAL is not discard eligible

class DEF2 has 5% bandwidth allocated
  the following protocols and filters are assigned:
    protocol ASRT with priority NORMAL is not discard eligible

assigned tags:

default class is DEFAULT with priority NORMAL

BRS [i 1] [dlci 17] Config>add-class 7
This circuit is currently using circuit defaults...
Are you sure you want to override the defaults?(Yes or [No]): yes
Class name [DEFAULT]? CIR171
Percent bandwidth to reserve [10]? 5
BRS[i 1] [dlci 17] Config>assign vines
Class name [DEFAULT]? CIR171
Priority <URGENT/HIGH/NORMAL/LOW> [NORMAL]?
Frame Relay Discard Eligible <NO/YES>[NO]?
```

Utilización de BRS y puesta en cola por prioridad

```
BRS [i 1] [dlci 17] Config>list
```

```
BANDWIDTH RESERVATION listing from SRAM  
bandwidth reservation is enabled  
interface number 1, circuit number 17  
maximum queue length 10, minimum queue length 3  
total bandwidth allocated 65%  
total classes defined (counting one local and one default) 5
```

```
class LOCAL has 10% bandwidth allocated  
  protocols and filters cannot be assigned to this class.
```

```
class DEFAULT has 40% bandwidth allocated  
  the following protocols and filters are assigned:  
    protocol ARP with default priority is not discard eligible  
    protocol DNA with default priority is not discard eligible  
    protocol IPX with default priority is not discard eligible  
    protocol OSI with default priority is not discard eligible  
    protocol VOFR with default priority is not discard eligible  
    protocol AP2 with default priority is not discard eligible
```

```
class DEF1 has 5% bandwidth allocated  
  the following protocols and filters assigned:  
    protocol IP with priority NORMAL is not discard eligible
```

```
class DEF2 has 5% bandwidth allocated  
  the following protocols and filters are assigned:  
    protocol ASRT with priority NORMAL is not discard eligible
```

```
class CIRC171 has 5% bandwidth allocated  
  the following protocols and filters are assigned:  
    protocol VINES with priority NORMAL is not discard eligible
```

```
assigned tags:
```

```
default class is DEFAULT with priority NORMAL
```

```
BRS [i 1] [dlci 17] Config>show
```

```
BANDWIDTH RESERVATION currently in RAM  
interface number 1, circuit number 17  
maximum queue length 10, minimum queue length 3  
5 current defined classes:  
  class LOCAL has 10% bandwidth allocated  
  class DEFAULT has 40% bandwidth allocated  
  class DEF1 has 5% bandwidth allocated  
  class DEF2 has 5% bandwidth allocated  
  class CIRC171 has 5% bandwidth allocated
```

Utilización de BRS y puesta en cola por prioridad

protocol and filter assignments:

Protocol/Filter	Class	Priority	Discard Eligible
-----	----	-----	-----
IP	DEF1	NORMAL	NO
ARP	DEFAULT	NORMAL	NO
DNA	DEFAULT	NORMAL	NO
VINES	CIRC171	NORMAL	NO
IPX	DEFAULT	NORMAL	NO
OSI	DEFAULT	NORMAL	NO
VOFR	DEFAULT	NORMAL	NO
AP2	DEFAULT	NORMAL	NO
ASRT	DEF2	NORMAL	NO

```
BRS [i 1] [d1ci 17] Config>exit
BRS [i 1] Config>set-circuit-defaults
BRS [i 1] [circuit defaults] Config>change DEF1 8
Percent bandwidth to reserve [ 5]? 10
BRS [i 1] [circuit defaults] Config>change DEF2
Percent bandwidth to reserve [5]? 10
BRS [i 1] [circuit defaults] Config>list
```

```
BANDWIDTH RESERVATION listing from SRAM
bandwidth reservation is enabled
interface number 1, default circuit
total bandwidth allocated 70%
total classes defined (counting one local and one default) 4
```

```
class LOCAL has 10% bandwidth allocated
  protocols and filters cannot be assigned to this class.
```

```
class DEFAULT has 40% bandwidth allocated
  the following protocols and filters are assigned:
  protocol ARP with default priority is not discard eligible
  protocol DNA with default priority is not discard eligible
  protocol VINES with default priority is not discard eligible
  protocol IPX with default priority is not discard eligible
  protocol OSI with default priority is not discard eligible
  protocol VOFR with default priority is not discard eligible
  protocol AP2 with default priority is not discard eligible
```

```
class DEF1 has 10% bandwidth allocated
  the following protocols and filters are assigned:
  protocol IP with priority NORMAL is not discard eligible
```

```
class DEF2 has 10% bandwidth allocated
  the following protocols and filters are assigned:
  protocol ASRT with priority NORMAL is not discard eligible
```

assigned tags:

```
default class is DEFAULT with priority NORMAL
```

```
BRS [i 1] [circuit defaults] Config>exit
```


Utilización de BRS y puesta en cola por prioridad

```
BRS [i 1] Config>circuit 16
BRS [i 1] [dlci 16] Config>list

BANDWIDTH RESERVATION listing from SRAM
bandwidth reservation is enabled
interface number 1, circuit number 16 using defaults.
maximum queue length 10, minimum queue length 3
total bandwidth allocated 70%
total classes defined (counting one local and one default) 4

class LOCAL has 10% bandwidth allocated
  protocols and filters cannot be assigned to this class.

class DEFAULT has 40% bandwidth allocated
  the following protocols and filters are assigned:
    protocol ARP with default priority is not discard eligible
    protocol DNA with default priority is not discard eligible
    protocol VINES with default priority is not discard eligible
    protocol IPX with default priority is not discard eligible
    protocol OSI with default priority is not discard eligible
    protocol VOFR with default priority is not discard eligible
    protocol AP2 with default priority is not discard eligible

class DEF1 has 10% bandwidth allocated
  the following protocols and filters are assigned:
    protocol IP with priority NORMAL is not discard eligible

class DEF2 has 10% bandwidth allocated
  the following protocols and filters are assigned:
    protocol ASRT with priority NORMAL is not discard eligible

assigned tags:

default class is DEFAULT with priority NORMAL

BRS [i 1] [dlci 16] Config>exit
```

Utilización de BRS y puesta en cola por prioridad

```
BRS [i 1] Config>circuit 17
BRS [i 1] [d1ci 17] Config>list

BANDWIDTH RESERVATION listing from SRAM
bandwidth reservation is enabled
interface number 1, circuit number 17
maximum queue length 10, minimum queue length 3
total bandwidth allocated 65%
total classes defined (counting one local and one default) 5

class LOCAL has 10% bandwidth allocated
  protocols and filters cannot be assigned to this class.

class DEFAULT has 40% bandwidth allocated
  the following protocols and filters are assigned:
    protocol ARP with default priority is not discard eligible
    protocol DNA with default priority is not discard eligible
    protocol IPX with default priority is not discard eligible
    protocol OSI with default priority is not discard eligible
    protocol VOFR with default priority is not discard eligible
    protocol AP2 with default priority is not discard eligible

class DEF1 has 5% bandwidth allocated
  the following protocols and filters are assigned:
    protocol IP with priority NORMAL is not discard eligible

class DEF2 has 5% bandwidth allocated
  the following protocols and filters are assigned:
    protocol ASRT with priority NORMAL is not discard eligible

class CIRC171 has 5% bandwidth allocated
  the following protocols and filters are assigned:
    protocol VINES with priority NORMAL is not discard eligible

assigned tags:

default class is DEFAULT with priority NORMAL

BRS [i 1] [d1ci 17] Config>use-circuit-defaults 9
This circuit is currently NOT using circuit defaults...
Are you sure you want to delete current definitions and use defaults ? (Yes or
[No]): yes
Defaults are in effect for this circuit.
Please reload router for this command to take effect.
BRS [i 1] [d1ci 17] Config>
*restart
Are you sure you want to reload the gateway? (Yes or [No] ):yes
```

```

*t 6
Gateway user configuration
Config>feature brs
Bandwidth Reservation User Configuration
BRS Config>interface 1
BRS [i 1] Config>circuit 17
BRS [i 1] [dlci 17] Config>list

BANDWIDTH RESERVATION listing from SRAM
bandwidth reservation is enabled
interface number 1, circuit number 17 using defaults.
maximum queue length 10, minimum queue length 3
total bandwidth allocated 70%
total classes defined (counting one local and one default) 4

class LOCAL has 10% bandwidth allocated
  protocols and filters cannot be assigned to this class.

class DEFAULT has 40% bandwidth allocated
  the following protocols and filters are assigned:
    protocol ARP with default priority is not discard eligible
    protocol DNA with default priority is not discard eligible
    protocol VINES with default priority is not discard eligible
    protocol IPX with default priority is not discard eligible
    protocol OSI with default priority is not discard eligible
    protocol VOFR with default priority is not discard eligible
    protocol AP2 with default priority is not discard eligible

class DEF1 has 10% bandwidth allocated
  the following protocols and filters are assigned:
    protocol IP with priority NORMAL is not discard eligible

class DEF2 has 10% bandwidth allocated
  the following protocols and filters are assigned:
    protocol ASRT with priority NORMAL is not discard eligible

assigned tags:

default class is DEFAULT with priority NORMAL

BRS [i 1] [dlci 17] Config>show

BANDWIDTH RESERVATION currently in RAM
interface number 1, circuit number 17 using defaults.
maximum queue length 10, minimum queue length 3
4 current defined classes:
  class LOCAL has 10% bandwidth allocated
  class DEFAULT has 40% bandwidth allocated
  class DEF1 has 10% bandwidth allocated
  class DEF2 has 10% bandwidth allocated

protocol and filter assignments:

```

Protocol/Filter	Class	Priority	Discard Eligible
IP	DEF1	NORMAL	NO
ARP	DEFAULT	NORMAL	NO
DNA	DEFAULT	NORMAL	NO
VINES	DEFAULT	NORMAL	NO
IPX	DEFAULT	NORMAL	NO
OSI	DEFAULT	NORMAL	NO
VOFR	DEFAULT	NORMAL	NO
AP2	DEFAULT	NORMAL	NO
ASRT	DEF2	NORMAL	NO

```

BRS [i 1] [dlci 17] Config>exit

```

Utilización de BRS y puesta en cola por prioridad

Configuración y supervisión de reserva de ancho de banda

Este capítulo describe los mandatos operativos y de configuración del Sistema de reserva de ancho de banda (BRS).

Este capítulo incluye las secciones siguientes:

- “Visión general de la configuración de la reserva de ancho de banda”
- “Mandatos de configuración de reserva de ancho de banda” en la página 26
- “Acceso al indicador de supervisión de la reserva de ancho de banda” en la página 50
- “Mandatos de supervisión de reserva de ancho de banda” en la página 51

Visión general de la configuración de la reserva de ancho de banda

Para acceder a los mandatos de configuración de la reserva de ancho de banda y configurar la reserva de ancho de banda en el direccionador:

1. En el indicador OPCON (*), entre **talk 6**.
2. En el indicador Config>, entre **feature brs**.
3. En el indicador BRS Config>, entre **interface #**.
4. En el indicador BRS [i 0] Config>, entre **enable**.

Éste es el nivel del indicador de interfaz y el número de interfaz es cero en este caso. Tiene que repetir los pasos 3 y 4 para cada interfaz que se está configurando.

Si configura BRS en una interfaz Frame Relay, continúe con el paso 4a:

Si configura BRS en cualquier otra interfaz, vaya directamente al paso 5.

- a. En el indicador BRS [i 0] Config>, entre **circuit #**, donde # es el número del circuito que se desea configurar.
 - b. En el indicador BRS [i 0] [dlci 16] Config>, entre **enable**. Éste es el nivel del indicador de circuito y el número de circuito (DLCI) es 16 en este caso.
 - c. En el indicador BRS [i 0] [dlci 16] Config>, entre **exit** para regresar al indicador de nivel de interfaz.
 - d. Repita los pasos 4a a 4c para cada circuito para el que desea definir clases-t BRS.
5. Vuelva a cargar el direccionador.
 6. Repita los pasos 1 a 3 para configurar la reserva de ancho de banda para la interfaz específica que ha habilitado.
 7. Si configura BRS en una interfaz PPP, en el indicador BRS[i 0]Config>, configure las clases de tráfico y asigne los protocolos, filtros y códigos a las clases de tráfico mediante los mandatos de configuración que aparecen listados en la Tabla 4 en la página 29. Si configura BRS en una interfaz FR, siga los pasos 8 a 10.
 8. Si configura BRS en una interfaz FR, puede configurar clases de circuito y asignar circuitos a clases de circuito mediante los mandatos que aparecen listados en la Tabla 3 en la página 28

Configuración de BRS y puesta en colas de prioridad

9. Si desea utilizar las definiciones de circuito por omisión, entre el mandato **set-circuit-defaults** en el indicador `BRS[i 0]Config>`. Esta acción le conducirá al indicador `BRS[i 0][circuit defaults]`, donde podrá utilizar los mandatos adecuados de la Tabla 4 en la página 29 para configurar las clases de tráfico y asignar protocolos, filtros y códigos a las clases de tráfico. Una vez que haya acabado de establecer las definiciones de circuito por omisión para la gestión de clases de tráfico, entre "exit" para regresar al indicador `BRS[i 0] Config>`.
10. Si tiene circuitos FR que no pueden utilizar las definiciones de circuito por omisión para la gestión de clases de tráfico, entre **circuit** *circuito-virtual-permanente número_circuito*. Así accederá al indicador de circuito, donde podrá utilizar los mandatos que aparecen listados en la Tabla 4 en la página 29 para crear definiciones específicas de circuito para la gestión de clases de tráfico.

Nota: No es necesario que recargue el direccionador para que los cambios de configuración de clase-t y clase-c entren en vigor.

El mandato **talk 6 (t 6)** le permite acceder al proceso de configuración.

El mandato **feature brs** le permite acceder al proceso de configuración de BRS. Puede entrar este mandato utilizando el nombre (brs) o el número (1) de la característica.

El mandato **interface #** selecciona la interfaz específica que desea configurar para la reserva de ancho de banda. Antes de configurar clases de BRS, debe utilizar el mandato **enable** para habilitar BRS en la interfaz. En el paso 4 en la página 25, el indicador señala que el número de la interfaz seleccionada es cero.

El mandato **circuit #** selecciona el circuito en la interfaz FR en la que desea configurar clases de tráfico BRS. Antes de configurar clases-t BRS para el circuito, debe utilizar el mandato **enable** para habilitar BRS en el circuito. En el paso 4b en la página 25, el indicador señala que se ha seleccionado el circuito 16 en la interfaz 0.

Debe habilitar la reserva de ancho de banda para la interfaz y el circuito seleccionados y, a continuación, volver a cargar el direccionador antes de configurar clases de circuito (sólo Frame Relay) y clases de tráfico.

Para regresar al indicador `Config>` en cualquier momento, entre el mandato **exit** en los distintos niveles de indicadores BRS hasta que se encuentre en el indicador `Config>`.

Mandatos de configuración de reserva de ancho de banda

En esta sección se describen los mandatos de configuración de la Reserva de ancho de banda. Los mandatos que pueden utilizarse difieren, según el indicador de configuración de BRS que se visualiza (`BRS Config>`, `BRS [i x] Config>`, o `BRS [i x] [dlci y] Config>`, o `BRS [i x] [circuit defaults] Config>`).

Tabla 2 (Página 1 de 2). Resumen de mandatos de configuración de la reserva de ancho de banda (disponible en el indicador BRS Config>)

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxiv.
Activate-IP-precedence-filtering	Activa el filtrado de precedencia BRS IPv4 de los paquetes APPN y SNA que se envían a través de un túnel IP seguro o que están en fragmentos TCP o UDP secundarios. Debe configurar también el valor de los bits de precedencia IPv4 cuando configure DLSw, HPR a través de IP o TN3270.
Deactivate-IP-precedence-filtering	Desactiva el proceso de filtrado de precedencia IPv4.
Enable-hpr-over-ip-port-numbers	Habilita la utilización del filtrado BRS para el tráfico APPN-HPR a través de IP y permite la configuración de los números de puerto UDP utilizados para identificar paquetes HPR a través de IP. Nota: Si APPN está en la imagen de carga, este mandato no está soportado, ya que BRS aprende de APPN si se ha configurado HPR a través de IP y, en caso afirmativo, aprende los números de puerto UDP que se utilizarán para los paquetes HPR a través de IP del soporte APPN.
Disable-hpr-over-ip-port-numbers	Inhabilita el filtrado BRS del tráfico APPN-HPR a través de IP. Nota: Si APPN está en la imagen de carga, este mandato no está soportado, ya que BRS aprende de APPN si se ha configurado HPR a través de IP o no.
Interface	Selecciona una interfaz en la que se configurará la reserva de ancho de banda. Nota: Debe entrarse este mandato antes de utilizar otros mandatos de configuración. Vea la Tabla 3 en la página 28 y la Tabla 4 en la página 29.

Configuración de BRS y puesta en colas de prioridad

Tabla 2 (Página 2 de 2). Resumen de mandatos de configuración de la reserva de ancho de banda (disponible en el indicador BRS Config>)

Mandato	Función
List	Lista las interfaces que pueden dar soporte a la reserva de ancho de banda y, para cada interfaz, indica si la reserva de ancho de banda está habilitada o inhabilitada.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiv.

Tabla 3 (Página 1 de 2). Mandatos de configuración de interfaz BRS disponibles en el indicador BRS [i #] Config> para interfaces Frame Relay

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxiv.
Add-circuit-class	Define el nombre de una clase-c de ancho de banda y su porcentaje de ancho de banda.
Assign-circuit	Asigna un circuito especificado a la clase-c de ancho de banda especificada.
Change-circuit-class	Cambia la cantidad de ancho de banda configurada para una clase-c de ancho de banda.
Circuit	Accede al indicador BRS de nivel de circuito (BRS [i x] [dlci y] Config>), donde puede utilizar los mandatos que aparecen listados en la Tabla 4 en la página 29 para configurar la Reserva de ancho de banda en el circuito Frame Relay.
Clear-block	Borra los datos de configuración asociados a la interfaz actual de SRAM. Se borran los datos de la configuración de clase de circuito y las definiciones de circuito por omisión para la gestión de clases de tráfico.
Deassign-circuit	Restaura el circuito especificado a la clase-c por omisión.
Default-circuit-class	Asigna el nombre de una clase-c de ancho de banda por omisión y su porcentaje del ancho de banda de la interfaz.
Del-circuit-class	Suprime la clase-c de ancho de banda especificada.
Disable	Inhabilita la reserva de ancho de banda en la interfaz.
Enable	Habilita la reserva de ancho de banda en la interfaz.
List	Visualiza las clases-c y las definiciones de circuito asignadas de SRAM.
Queue-length	Define los valores máximo y mínimo para el número de paquetes en una cola de prioridad.
Set-circuit-defaults	Accede al indicador de mandatos BRS [i x] [circuit defaults] Config> para que pueda utilizar los mandatos adecuados de la Tabla 4 en la página 29 para crear definiciones de circuito por omisión para la gestión de clases de tráfico.

Tabla 3 (Página 2 de 2). Mandatos de configuración de interfaz BRS disponibles en el indicador BRS [i #] Config> para interfaces Frame Relay

Mandato	Función
Show	Visualiza las clases-c definidas actualmente y los circuitos asignados de SRAM.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiv.

La tabla siguiente lista los mandatos de circuitos BRS disponibles en BRS [i x] Config> para las interfaces PPP, en el indicador BRS [i x] dlci [y] Config> para circuitos Frame Relay y en el indicador BRS [i x] [circuit defaults] Config>.

Tabla 4 (Página 1 de 2). Mandatos de gestión de clases de tráfico BRS

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxiv.
Add-class	Asigna una cantidad designada de ancho de banda a una clase de tráfico definida por el usuario.
Create-super-class	Define la clase-t denominada <i>super-class</i> .
Assign	Asigna un protocolo o un filtro a una clase de tráfico configurada.
Change-class	Cambia la cantidad de ancho de banda configurada para una clase-t de ancho de banda.
Clear-block	Borra la clase de tráfico y los datos de configuración de las asignaciones de protocolos, filtros y códigos de SRAM para la interfaz PPP o el circuito Frame Relay. Nota: Este mandato no se puede utilizar en el indicador BRS [i x] [circuit defaults] Config>.
Deassign	Restaura la puesta en cola del paquete o filtro especificado a la clase-t y la prioridad por omisión.
Default-class	Define la clase-t y la prioridad por omisión como un valor deseado y asigna todos los protocolos no asignados a la nueva clase-t por omisión.
Del-class	Suprime una clase-t de ancho de banda configurada anteriormente.
Disable	Inhabilita la reserva de ancho de banda en la interfaz PPP o en el circuito Frame Relay. Nota: BRS no se puede habilitar o inhabilitar en el indicador BRS [i x] [circuit defaults] Config>.
Enable	Habilita la reserva de ancho de banda en la interfaz PPP o en el circuito Frame Relay. Nota: BRS no se puede habilitar o inhabilitar en el indicador BRS [i x] [circuit defaults] Config>.
List	Lista las clases-t configuradas y las asignaciones de protocolos, filtros y códigos almacenadas en SRAM.

Configuración de BRS y puesta en colas de prioridad

Mandato	Función
Queue-length	Define los valores máximo y mínimo para el número de paquetes en una cola de prioridad. Nota: Este mandato no está soportado en el indicador BRS [i x] [circuit defaults] Config>.
Show	Visualiza las clases-t definidas actualmente y las asignaciones de protocolos, filtros y códigos almacenadas en RAM. Nota: Este mandato no está soportado en el indicador BRS [i x] [circuit defaults] Config>.
Tag	Asigna un nombre de código BRS (TAG1 - TAG5) a un filtro MAC que se ha codificado durante la configuración de la característica Filtrado MAC.
Untag	Elimina la relación entre un nombre de código BRS (TAG1 - TAG5) y un filtro MAC que se ha codificado durante la configuración de la característica Filtrado MAC.
Use-circuit-defaults	Permite al usuario suprimir las definiciones específicas de circuito y utilizar las definiciones por omisión de circuitos para la gestión de clases de tráfico. Este mandato sólo es válido en el indicador BRS [i x] dlci [y] Config> para Frame Relay. Nota: El direccionador se debe volver a cargar para que los valores por omisión sean operativos.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página xxxiv.

Utilice los mandatos adecuados para configurar la reserva de ancho de banda para el protocolo PPP (Punto a punto) y Frame Relay. Para Frame Relay, tiene que configurar el circuito y la interfaz de red. Para PPP, sólo tendrá que configurar la interfaz de red.

Notas:

1. Cuando los mandatos **clear-block**, **disable**, **enable**, **list** y **show** se emiten desde el menú de interfaz de BRS, afectan a, o listan, la información de reserva de ancho de banda configurada para la interfaz seleccionada. Cuando se emiten estos mandatos desde el menú de circuito de BRS, sólo la información de reserva de ancho de banda de Frame Relay configurada para el circuito virtual permanente (PVC) se ve afectada o se lista.
2. Antes de utilizar los mandatos de reserva de ancho de banda, tenga en cuenta lo siguiente:
 - Debe utilizar el mandato **interface** para seleccionar una interfaz antes de utilizar ningún otro mandato de configuración. (La configuración de BRS obliga a esto.)
 - El parámetro *Nombre-clase* es sensible a las mayúsculas y minúsculas.
 - Para ver los *nombre-clase* actuales, utilice el mandato **list** o **show**.
 - Después de habilitar la reserva de ancho de banda en una interfaz o un circuito, puede añadir/suprimir/cambiar clases de circuitos y tráficos y asignar circuitos o protocolos dinámicamente. Los únicos mandatos que

requieren que un direccionador se vuelva a cargar antes de entrar en vigor son los mandatos `enable`, `disable`, `use-circuit-defaults` y `clear-block`.

3. No es necesario que vuelva a cargar el direccionador para que los cambios de configuración de clase-t y clase-c entren en vigor.

Activate-IP-precedence-filtering

Utilice el mandato **activate-ip-precedence-filtering** para activar el filtrado de precedencia BRS IPv4 de paquetes APPN y SNA que se envían a través de un túnel IP seguro o que están en fragmentos TCP o UDP secundarios. Debe configurar también el valor de los bits de precedencia IPv4 cuando configure DLSw, HPR a través de IP o TN3270. Consulte “Utilización del proceso de bits de precedencia de IP Versión 4 para el tráfico SNA en túneles seguros IP y fragmentos secundarios” en la página 10 para obtener más información.

Sintaxis:

activate-ip-precedence-filtering

Add-circuit-class

Nota: Sólo se utiliza al configurar Frame Relay.

Utilice el mandato **add-circuit-class** al nivel de interfaz para asignar una cantidad designada de ancho de banda que utilizará el grupo de circuitos asignado a la clase-c de ancho de banda definida por el usuario.

Sintaxis:

add-circuit-class *nombre-clase* %

Add-class

Utilice el mandato **add-class** para asignar una cantidad designada de ancho de banda a una clase-t de ancho de banda definida por el usuario.

Nota: Si este mandato se utiliza para un circuito Frame Relay que utiliza actualmente definiciones de circuito por omisión para la gestión de clases de tráfico, se le preguntará si desea alterar temporalmente las definiciones de circuito por omisión. Si responde “Yes”, el circuito cambiará para utilizar definiciones específicas de circuito para la gestión de clases de tráfico y se permitirá el mandato. Si responde “No”, el mandato terminará anormalmente y se seguirán utilizando las definiciones de circuito por omisión para el circuito. Si desea modificar las definiciones de circuito por omisión, debe dirigirse al indicador de mandatos BRS `[i x][circuit defaults]Config>`.

Sintaxis:

add-class [*nombre-clase* o *núm-clase*] %

Ejemplo 1: Adición de una clase denominada CIRC17 en un circuito Frame Relay

```
BRS [i 1] [dlci 17] Config>add-class
This circuit is currently using circuit defaults...
Are you sure you want to override the defaults?(Yes or [No]):y
Class name [DEFAULT]? CIRC17
Percent bandwidth to reserve [10]?5
BRS [i 1] [dlci 17] Config>list
```

```
BANDWIDTH RESERVATION listing from SRAM
bandwidth reservation is enabled
interface number 1, circuit number 17
maximum queue length 10, minimum queue length 3
total bandwidth allocated 65%
total classes defined (counting one local and one default) 5
```

```
class LOCAL has 10% bandwidth allocated
  protocols and filters cannot be assigned to this class.
```

```
class DEFAULT has 40% bandwidth allocated
  the following protocols and filters are assigned:
  protocol DNA with default priority is not discard eligible
  protocol VINES with default priority is not discard eligible
  protocol IPX with default priority is not discard eligible
  protocol OSI with default priority is not discard eligible
  protocol VOFR with default priority is not discard eligible
  protocol AP2 with default priority is not discard eligible
  protocol ASRT with default priority is not discard eligible
```

```
class DEF1 has 5% bandwidth allocated
  protocol IP with priority NORMAL is not discard eligible.
```

```
class DEF2 has 5% bandwidth allocated
  protocol ARP with priority NORMAL is not discard eligible.
```

```
class CIRC171 has 5% bandwidth allocated
  no protocols or filters are assigned to this class.
```

```
assigned tags:
```

```
default class is DEFAULT with priority NORMAL
```

Ejemplo 2: Adición de una clase denominada class1 en un circuito Frame Relay

```
BRS [i 2] [d1ci 128]>add
This circuit is currently using circuit defaults...
Are you sure you want to override the defaults?(Yes or [No]): y
Class name [DEFAULT]?
Class is already allocated.
BRS [i 2] [d1ci 128]>add class1
Percent bandwidth to reserve [10]?
BRS [i 2] [d1ci 128]>
```

```
BRS [i 2] [d1ci 128]>list
```

```
BANDWIDTH RESERVATION listing from SRAM
bandwidth reservation is enabled
interface number 2, circuit number 128
maximum queue length 10, minimum queue length 3
total bandwidth allocated 60%
total classes defined (counting one local and one default) 3
```

```
class LOCAL has 10% bandwidth allocated
  protocols and filters cannot be assigned to this class.
```

```
class DEFAULT has 40% bandwidth allocated
  the following protocols and filters are assigned:
  protocol IP with default priority is not discard eligible
  protocol ARP with default priority is not discard eligible
  protocol DNA with default priority is not discard eligible
  protocol VINES with default priority is not discard eligible
  protocol IPX with default priority is not discard eligible
  protocol OSI with default priority is not discard eligible
  protocol VOFR with default priority is not discard eligible
  protocol AP2 with default priority is not discard eligible
  protocol ASRT with default priority is not discard eligible
```

```
class class1 has 10% bandwidth allocated
  no protocols or filters are assigned to this class.
```

```
assigned tags:
```

```
default class is DEFAULT with priority NORMAL
```

```
BRS [i 2] [d1ci 128]>
```

Assign

Utilice el mandato **assign** para asignar códigos, paquetes de protocolos o filtros especificados a una clase-t y una prioridad dadas en esa clase. Los cuatro tipos de prioridad son:

- Urgent
- High
- Normal (prioridad por omisión)
- Low.

Nota: Se utiliza el protocolo VOFR (Voz a través de Frame Relay) cuando los paquetes de voz se envían a través de una interfaz Frame Relay. Si un circuito sólo transportará paquetes de voz, sólo asignará una clase-t en el circuito y especificará el protocolo como VOFR. Sólo se permite una clase-t, porque una clase-t no tiene prioridad sobre otra. Si hay más de una clase-t, una clase-t que no transporte voz puede obtener el control del ancho de banda e interferir con la transmisión del tráfico de voz. Para ase-

Configuración de BRS y puesta en colas de prioridad

gurar que el tráfico de voz recibirá una transmisión inmediata, al tráfico VOFR sólo se le debe dar el tipo de prioridad *Urgent*.

Es preciso configurar en el circuito la fragmentación a través de Frame Relay, tal como se describe en el mandato **enable fragmentation** command en el capítulo “Configuring and Monitoring Frame Relay Interfaces” del manual *Nways Multiprotocol Access Services Guía del usuario de software*, si transportará tráfico de datos y voz. Esto es necesario para que paquetes grandes de datos no utilicen todo el ancho de banda e impidan así que los paquetes de voz pasen lo bastante deprisa.

Sintaxis:

assign [clase-protocolo o TAG o clase-filtro] [nombre-clase o núm-clase]

El mandato **assign** le permite también definir el bit DE (Elegible para eliminación) para tramas Frame Relay.

Nota: Si este mandato se utiliza para un circuito Frame Relay que utiliza actualmente definiciones de circuito por omisión para la gestión de clases de tráfico, se le preguntará si desea alterar temporalmente las definiciones de circuito por omisión. Si responde “Yes”, el circuito cambiará para utilizar definiciones específicas de circuito para la gestión de clases de tráfico y se permitirá el mandato. Si responde “No”, el mandato terminará anormalmente y se seguirán utilizando las definiciones de circuito por omisión para el circuito. Si desea modificar las definiciones de circuito por omisión, debe dirigirse al indicador de mandatos BRS [i x][circuit defaults]Config>.

Ejemplo 1:

```
assign IPX test
priority <URGENT/HIGH/NORMAL/LOW>: [NORMAL]? low
protocol IPX maps to class test with priority LOW Discard eligible <yes/no> [N]?
```

Ejemplo 2: Asignación de un filtro TOS a class1; class1 se ha añadido previamente a la configuración mediante el mandato `add class`.

```
BRS [i 2] [d1ci 128]>assign ?
IP
ARP
DNA
VINES
IPX
OSI
VOFR
AP2
ASRT
TUNNELING-IP
SDLC/BSC-IP
RLOGIN-IP
TELNET-IP
NETBIOS
SNA/APPN-ISR
SNMP-IP
MULTICAST-IP
DLSW-IP
TAG1
TAG2
TAG3
TAG4
TAG5
APPN-HPR
NETWORK-HPR
HIGH-HPR
MEDIUM-HPR
LOW-HPR
XTP-IP
UDP_TCP1
UDP_TCP2
UDP_TCP3
UDP_TCP4
UDP_TCP5
TOS1
TOS2
TOS3
TOS4
TOS5
Protocol or filter name [IP]? TOS1 1
Class name [DEFAULT]? class1 2
Priority [NORMAL]?
Frame Relay Discard Eligible [NO]?
TOS Mask [1-FF] [FF]?
TOS Range (Low) [0-FF] [0]? 1
TOS Range (High) [1]? 3
BRS [i 2] [d1ci 128]> list

BANDWIDTH RESERVATION listing from SRAM
bandwidth reservation is enabled
interface number 2, circuit number 128
maximum queue length 10, minimum queue length 3
total bandwidth allocated 60%
total classes defined (counting one local and one default) 3

class LOCAL has 10% bandwidth allocated
  protocols and filters cannot be assigned to this class.
```

Configuración de BRS y puesta en colas de prioridad

```
class DEFAULT has 40% bandwidth allocated
  the following protocols and filters are assigned:
    protocol IP with default priority is not discard eligible
    protocol ARP with default priority is not discard eligible
    protocol DNA with default priority is not discard eligible
    protocol VINES with default priority is not discard eligible
    protocol IPX with default priority is not discard eligible
    protocol OSI with default priority is not discard eligible
    protocol VOFR with default priority is not discard eligible
    protocol AP2 with default priority is not discard eligible
    protocol ASRT with default priority is not discard eligible
```

```
class class1 has 10% bandwidth allocated
  the following protocols and filters are assigned:
    filter TOS1 with priority NORMAL is not discard eligible
      with TOS range x1 - x3 and TOS mask xFF
```

assigned tags:

default class is DEFAULT with priority NORMAL

```
BRS [i 2] [dlci 128]>show
```

```
BANDWIDTH RESERVATION currently in RAM
interface number 2, circuit number 128
maximum queue length 10, minimum queue length 3
3 current defined classes:
  class LOCAL has 10% bandwidth allocated
  class DEFAULT has 40% bandwidth allocated
  class class1 has 10% bandwidth allocated
```

protocol and filter assignments:

Protocol/Filter	Class	Priority	Discard Eligible
-----	-----	-----	-----
IP	DEFAULT	NORMAL	NO
ARP	DEFAULT	NORMAL	NO
DNA	DEFAULT	NORMAL	NO
VINES	DEFAULT	NORMAL	NO
IPX	DEFAULT	NORMAL	NO
OSI	DEFAULT	NORMAL	NO
VOFR	DEFAULT	NORMAL	NO
AP2	DEFAULT	NORMAL	NO
ASRT	DEFAULT	NORMAL	NO
TOS1	class1	NORMAL	NO
	with TOS range x1 - x3		
	and TOS mask xFF		

```
BRS [i 2] [dlci 128]>
```

1 La utilización del filtro TOS requiere que entre tres parámetros: TOS mask, TOS range-low, y TOS range-high. Consulte el mandato “Add” en el capítulo “Configuring and Monitoring IP” del manual *Consulta de configuración y supervisión de protocolos Volumen 1* para obtener una descripción de estos parámetros.

Assign-circuit

Nota: Sólo se utiliza al configurar Frame Relay.

Utilice el mandato **assign-circuit** al nivel de interfaz para asignar el circuito especificado a la clase-c de ancho de banda especificada. Utilice la DLCI al asignar un PVC a una clase de circuito y el nombre de circuito al asignar un SVC a una clase de circuito.

Nota: Debe utilizar el mandato **circuit** para habilitar BRS en el circuito virtual y volver a cargar el direccionador antes de que pueda utilizar este mandato para asignar el circuito a una clase de circuito.

Sintaxis:

assign-circuit # *nombre clase*

Change-circuit-class

Nota: Sólo se utiliza al configurar Frame Relay.

Utilice el mandato **change-circuit-class** al nivel de interfaz para cambiar el porcentaje del ancho de banda que se utilizará por parte del grupo de circuitos asignado a la clase-c especificada.

Sintaxis:

change-circuit-class *nombre-clase* %

Change-class

Utilice el mandato **change-class** para modificar la cantidad de ancho de banda configurada para una clase-t de ancho de banda.

Nota: Si este mandato se utiliza para un circuito Frame Relay que utiliza actualmente definiciones de circuito por omisión para la gestión de clases de tráfico, se le preguntará si desea alterar temporalmente las definiciones de circuito por omisión. Si responde "Yes", el circuito cambiará para utilizar definiciones específicas de circuito para la gestión de clases de tráfico y se permitirá el mandato. Si responde "No", el mandato terminará anormalmente y se seguirán utilizando las definiciones de circuito por omisión para el circuito. Si desea modificar las definiciones de circuito por omisión, debe dirigirse al indicador de mandatos BRS [i x][circuit defaults]Config>.

Sintaxis:

change-class [*nombre-clase* o *núm-clase*] %

Circuit

Nota: Sólo se utiliza al configurar Frame Relay.

Utilice el mandato **circuit** para configurar un circuito virtual permanente (PVC) o un circuito virtual conmutado (SVC) Frame Relay. Este mandato sólo puede emitirse desde el indicador de configuración de interfaz BRS (BRS [i #] Config>).

Sintaxis:

circuit

Configuración de BRS y puesta en colas de prioridad

Antes de que pueda utilizar los mandatos **add-class**, **assign**, **default-class**, **del-class**, **deassign** o **change-class**, debe habilitar BRS en el circuito y volver a cargar el direccionador.

Ejemplo de PVC:

```
BRS [i 1] Config> circuit
Circuit (PVC number or SVC name) to reserve bandwidth: [16]

BRS [i 1 ] [dlci 16] Config> enable
```

Ejemplo de SVC:

```
BRS [i 1] Config> circuit
Circuit (PVC number or SVC name) to reserve bandwidth: [16] svc01

BRS [i 1 ] [svc svc01] Config> enable
```

Después de que se emita el mandato **enable** para el circuito Frame-Relay y el direccionador se vuelve a cargar, los siguientes mandatos de configuración estarán disponibles para el circuito:

add-class	deassign	enable	tag
assign	default-class	exit	untag
change-class	del-class	list	clear-block
disable	show	use-circuit-defaults	

Clear-block

Utilice el mandato **clear-block** para borrar de la SRAM los datos de configuración de reserva de ancho de banda actual.

Sintaxis:

clear-block

- Si entra este mandato desde el indicador de interfaz para PPP, todos los datos de configuración de BRS se borran de la interfaz.
- Si entra este mandato desde el indicador de interfaz para Frame Relay, BRS ya no estará habilitado en la interfaz o en cualquier circuito de la interfaz, y se borran todos los datos de configuración de clase de circuito y las definiciones de circuito por omisión para la gestión de clases de tráfico. No obstante, los datos de configuración de clases de tráfico para cada circuito individual no se borran y estarán disponibles si vuelve a habilitar BRS en la interfaz.
- Para borrar los datos de configuración de clase de tráfico del circuito, debe entrar en primer lugar el mandato **circuit** en el indicador de nivel de interfaz y, a continuación, el mandato **clear-block** en el indicador de nivel de circuito. Después de borrar los datos de configuración de clase de tráfico para cada circuito, entre el mandato **clear-block** en el indicador de nivel de interfaz para borrar los datos de configuración de clase de circuito. Los cambios no entran en vigor hasta que el direccionador no se vuelve a cargar.

Ejemplo:

```
clear-block
You are about to clear BRS configuration information for this interface
Are you sure you want to do this (Yes or No): y
BRS [i 1] Config>
```

Create-super-class

Utilice el mandato **create-super-class** para configurar una clase-t denominada *super-class* (superclase) en la interfaz PPP o en el circuito Frame Relay. Sólo puede configurarse una superclase para cada interfaz PPP en un circuito Frame Relay. No hay ningún porcentaje de ancho de banda asociado a la superclase. Cualquier dato de protocolo o de filtro que se asigne a una superclase se transmitirá antes que los datos de protocolo o de filtro asignados a cualquier otra clase-t en la interfaz PPP o en el circuito Frame Relay. Es preciso configurar una superclase para el protocolo VOFR (Voz a través de trama) para un circuito que transporte paquetes de voz y de datos. En este entorno, configurar la superclase para transportar voz ayudará a asegurar que los paquetes de voz obtengan prioridad.

Sintaxis:

create-super-class

Deactivate-IP-precedence-filtering

Utilice el mandato **deactivate-ip-precedence-filtering** para desactivar el proceso de filtrado de precedencia IPv4.

Sintaxis:

deactivate-ip-precedence-filtering

Deassign

Utilice el mandato **deassign** para restaurar la puesta en cola del paquete de protocolos o el filtro especificado en la clase-t y la prioridad por omisión.

Nota: Si este mandato se utiliza para un circuito Frame Relay que utiliza actualmente definiciones de circuito por omisión para la gestión de clases de tráfico, se le preguntará si desea alterar temporalmente las definiciones de circuito por omisión. Si responde "Yes", el circuito cambiará para utilizar definiciones específicas de circuito para la gestión de clases de tráfico y se permitirá el mandato. Si responde "No", el mandato terminará anormalmente y se seguirán utilizando las definiciones de circuito por omisión para el circuito. Si desea modificar las definiciones de circuito por omisión, debe dirigirse al indicador de mandatos BRS [i x][circuit defaults]Config>.

Sintaxis:

deassign [clase-prot o clase-filtro]

Deassign-circuit

Nota: Sólo se utiliza al configurar Frame Relay.

Utilice el mandato **deassign-circuit** al nivel de interfaz para restaurar la puesta en cola del circuito especificado a la clase-c por omisión.

Sintaxis:

deassign-c número

Default-circuit-class

Nota: Sólo se utiliza al configurar Frame Relay.

Utilice el mandato **default-circuit-class** en el nivel de interfaz para definir el nombre definido por el usuario de la clase-c de ancho de banda por omisión y el porcentaje del ancho de banda asignado a esa clase de circuitos, incluidos los huérfanos, que no estén asignados a una clase-c de ancho de banda.

Sintaxis:

default-circuit-class *nombre-clase %*

Del-circuit-class

Nota: Sólo se utiliza al configurar Frame Relay.

Utilice el mandato **del-circuit-class** al nivel de interfaz para suprimir la clase-c de ancho de banda especificada.

Sintaxis:

del-circuit-class *nombre-clase*

Default-class

Utilice el mandato **default-class** para definir la clase-t y la prioridad por omisión con un valor deseado. Si no se ha asignado ningún valor anteriormente, se utilizan valores por omisión del sistema. De lo contrario, se utilizará el último valor asignado anteriormente.

Nota: Si este mandato se utiliza para un circuito Frame Relay que utiliza actualmente definiciones de circuito por omisión para la gestión de clases de tráfico, se le preguntará si desea alterar temporalmente las definiciones de circuito por omisión. Si responde "Yes", el circuito cambiará para utilizar definiciones específicas de circuito para la gestión de clases de tráfico y se permitirá el mandato. Si responde "No", el mandato terminará anormalmente y se seguirán utilizando las definiciones de circuito por omisión para el circuito. Si desea modificar las definiciones de circuito por omisión, debe dirigirse al indicador de mandatos BRS [i x] [circuit defaults] Config>.

Sintaxis:

default-cl *[nombre-clase o núm-clase] prioridad*

Del-class

Utilice el mandato **del-class** para suprimir una clase-t de ancho de banda configurada anteriormente desde la interfaz o el circuito especificado.

Nota: Si este mandato se utiliza para un circuito Frame Relay que utiliza actualmente definiciones de circuito por omisión para la gestión de clases de tráfico, se le preguntará si desea alterar temporalmente las definiciones de circuito por omisión. Si responde "Yes", el circuito cambiará para utilizar definiciones específicas de circuito para la gestión de clases de tráfico y se permitirá el mandato. Si responde "No", el mandato terminará anormalmente y se seguirán utilizando las definiciones de circuito por omisión para el circuito. Si desea modificar las definiciones de circuito por omisión,

debe dirigirse al indicador de mandatos BRS [i x][circuit defaults]Config>.

Sintaxis:

del-class [nombre-clase o núm-clase]

Disable

Utilice el mandato **disable** para inhabilitar la reserva de ancho de banda en la interfaz (si se entra en el indicador de interfaz) o en el circuito (si se entra en el indicador de circuito). Los cambios no entran en vigor hasta que el direccionador se vuelve a cargar.

Para verificar que la reserva de ancho de banda está inhabilitada, entre el mandato **list**.

Sintaxis:

disable

Disable-hpr-over-ip-port-numbers

Utilice el mandato **disable-hpr-over-ip-port-numbers** para inhabilitar el filtrado BRS de tráfico de HPR a través de IP.

Sintaxis:

disable-hpr-over-ip-port-numbers

Para verificar que el filtrado BRS de tráfico de HPR a través de IP, entre el mandato **list**.

Nota: Si se ha incluido APPN en la imagen de carga, configure si se utilizará el tráfico de HPR a través de IP en el indicador de mandatos APPN Config>.

Enable

Utilice el mandato **enable** para habilitar la reserva de ancho de banda en la interfaz (si se entra en el indicador de interfaz) o en el circuito (si se entra en el indicador de circuito). Los cambios no entran en vigor hasta que el direccionador se vuelve a cargar.

Sintaxis:

enable

Nota:

- Al configurar BRS en una interfaz PPP, emita el mandato **enable** en el indicador de la interfaz y, a continuación, vuelva a cargar el direccionador antes de configurar clases de tráfico y asignar protocolos y filtros a clases de tráfico.
- Cuando se habilita BRS inicialmente en un circuito Frame Relay, éste se inicializa para utilizar definiciones de circuito por omisión para la gestión de clases de tráfico. Emita el mandato **enable** en el indicador de interfaz y en el indicador de circuito de cada circuito para el que desea definir clases de tráfico. A continuación, vuelva a cargar el

Configuración de BRS y puesta en colas de prioridad

direccionador antes de configurar clases de circuito para las clases de interfaz y de tráfico para cada circuito. Por ejemplo:

```
t 6
Gateway user configuration
Config>f brs
Bandwidth Reservation User Configuration
BRS Config>interface 1
BRS [i 1] Config>enable
Please reload router for this command to take effect
BRS [i 1] Config>list

BANDWIDTH RESERVATION listing from SRAM
bandwidth reservation is enabled
interface number 1
maximum queue length 10, minimum queue length 3
total bandwidth allocated 10%
total circuit classes defined (counting one default) 1

class DEFAULT has 10% bandwidth allocated
no circuits are assigned to this class.

default class is DEFAULT

BRS [i 1] Config>circ 16
BRS [i 1] [d1ci 16] Config>enable
Defaults are in effect for this circuit.
Please reload router for this command to take effect.
BRS [i 1] [d1ci 16] Config>ex
Please reload router for this command to take effect.
BRS [i 1] [d1ci 16] Config>
```

Enable-hpr-over-ip-port-numbers

Utilice el mandato **enable-hpr-over-ip-port-numbers** para habilitar el filtrado BRS del tráfico de APPN-HPR a través de IP y configurar los números de puerto UDP que se utilizan para identificar los paquetes de HPR a través de IP.

Nota: Si se ha incluido APPN en la imagen de carga, habilite el tráfico de HPR a través de IP y especifique que los números de puerto UDP utilizados para el tráfico de HPR a través de IP en el indicador de mandatos APPN Config>.

Sintaxis:

enable-hpr-over-ip-port-numbers

Ejemplo:

```
BRS Config> enable-hpr-over-ip-port-numbers
XID exchange port number [12000]?
HPR net trans prio port number [12001]?
HPR high trans prio port number [12002]?
HPR medium trans prio port number [12003]?
HPR low trans prio port number [12004]?
```

XID exchange port number (Número de puerto de intercambio de XID)

Este parámetro especifica el número de puerto UDP que se va a utilizar para el intercambio de XID. Este número de puerto debe ser el mismo que el definido en otros dispositivos de la red.

Valores válidos: 1024 - 65535

Valor por omisión: 12000

Network priority port number (Número de puerto de prioridad de red)

Este parámetro especifica el número de puerto UDP que se va a utilizar para el tráfico de prioridad de la red. Este número de puerto debe ser el mismo que el definido en otros dispositivos de la red.

Valores válidos: 1024 - 65535

Valor por omisión: 12001

High exchange port number (Número de puerto de intercambio alto)

Este parámetro especifica el número de puerto UDP que se va a utilizar para el tráfico de prioridad alta. Este número de puerto debe ser el mismo que el definido en otros dispositivos de la red.

Valores válidos: 1024 - 65535

Valor por omisión: 12002

Medium exchange port number (Número de puerto de intercambio medio)

Este parámetro especifica el número de puerto UDP que se va a utilizar para el tráfico de prioridad media. Este número de puerto debe ser el mismo que el definido en otros dispositivos de la red.

Valores válidos: 1024 - 65535

Valor por omisión: 12003

Low exchange port number (Número de puerto de intercambio bajo)

Este parámetro especifica el número de puerto UDP que se va a utilizar para el tráfico de prioridad baja. Este número de puerto debe ser el mismo que el definido en otros dispositivos de la red.

Valores válidos: 1024 - 65535

Valor por omisión: 12004

Interface

Utilice el mandato **interface** para seleccionar la interfaz serie a la que se aplicarán los mandatos de configuración de reserva de ancho de banda. *La reserva de ancho de banda está soportada en los direccionadores que ejecutan las interfaces PPP (Protocolo punto a punto) y Frame Relay.*

Sintaxis:

interface *núm-interfaz*

Notas:

1. Para entrar mandatos de reserva de ancho de banda para una interfaz nueva, es preciso entrar este mandato **antes** de utilizar ningún otro mandato de configuración de reserva de ancho de banda. Si ha salido del indicador de reserva de ancho de banda y desea regresar para realizar modificaciones en la reserva de ancho de banda en una interfaz configurada previamente, en primer lugar se debe entrar este mandato de nuevo.
2. Si se utiliza WAN Restoral y BRS está configurado en una interfaz primaria, también debe configurarse BRS en la interfaz secundaria. Habitualmente, cuando se utiliza WAN Restoral, la interfaz secundaria adopta la identidad de la interfaz primaria. Esto no es cierto para BRS; por consiguiente, es preciso configurar BRS tanto en la interfaz primaria como en la secundaria.

Para habilitar la Reserva de ancho de banda en una interfaz determinada, en el indicador `BRS Config>`, entre el número de interfaz que da soporte al protocolo o característica específico. A continuación, puede utilizar el mandato de configuración **BRS enable** tal como se describe en este capítulo. Tras habilitar el número de

Configuración de BRS y puesta en colas de prioridad

interfaz, debe volver a cargar el 2216 para que el mandato entre en vigor antes de que pueda realizar otros cambios de configuración en la interfaz.

Notas:

1. Si configura BRS en una interfaz Frame Relay, puede utilizar el mandato **circuit** para seleccionar circuitos y habilitar en ellos la reserva de ancho de banda antes de que vuelva a cargar el direccionador.

List

Utilice el mandato **list** para visualizar las clases de ancho de banda definidas actualmente y sus porcentajes garantizados.

Los mandatos **list** y **show** son similares. El mandato **list** visualiza las definiciones actuales de la SRAM, mientras que el mandato **show** visualiza las definiciones actuales de la RAM.

Sintaxis:

list *núm-interfaz*

Según el indicador en el que se emita el mandato **list**, se visualizarán diversas salidas. Puede emitir el mandato **list** desde los indicadores siguientes:

- BRS [i 1] [dlci 16] Config>
- BRS [i 1] Config>
- BRS Config>
- BRS [i 1] [circuit defaults] Config>

Nota: Cuando se utiliza este mandato en un indicador de circuito Frame Relay (BRS [i x] [dlci y] Config>), indica si el circuito utiliza definiciones de circuito por omisión o definiciones específicas de circuito para la gestión de clases de tráfico. Si el circuito utiliza definiciones de circuito por omisión, se visualizan las asignaciones de clases de tráfico, protocolos, filtros y códigos definidos actualmente para las definiciones de circuito por omisión. No obstante, si desea alterar las definiciones de circuito por omisión, tiene que dirigirse al indicador BRS[i x] [circuit defaults] Config> para efectuar los cambios.

En el indicador de nivel de interfaz BRS (BRS [i 0]) para las interfaces PPP y en el indicador de nivel de circuito BRS (BRS [i 0] [dlci 16] Config>) para las interfaces Frame Relay, el mandato **list** genera una lista de clases de tráfico, sus porcentajes configurados de ancho de banda y los protocolos y filtros asignados.

En el indicador de nivel de interfaz BRS para Frame Relay, el mandato **list** genera una lista de las clases de circuito, sus porcentajes configurados de ancho de banda y los circuitos asignados.

Ejemplo 1

```
BRS Config>list
Bandwidth Reservation is available for 2 interfaces.

Interface   Type      State
-----
1          FR       Enabled
2          PPP      Enabled

The use of HPR over IP port numbers is disabled

BRS Config>interface 1
BRS [i 1] Config>list

BANDWIDTH RESERVATION listing from SRAM
bandwidth reservation is enabled
interface number 1
maximum queue length 10, minimum queue length 3
total bandwidth allocated 10%
total circuit classes defined (counting one default) 1

class DEFAULT has 10% bandwidth allocated
the following circuits are assigned:
  17
  16 using defaults.
  18 using defaults.

default class is DEFAULT

BRS [i 2] Config>exit
BRS Config>interface 2
BRS [i 2] Config>list

BANDWIDTH RESERVATION listing from SRAM
bandwidth reservation is enabled
interface number 2
maximum queue length 10, minimum queue length 3
total bandwidth allocated 50%
total classes defined (counting one local and one default) 2

class LOCAL has 10% bandwidth allocated
protocols and filters cannot be assigned to this class.

class DEFAULT has 40% bandwidth allocated
the following protocols and filters are assigned:
protocol IP with default priority
protocol ARP with default priority
protocol DNA with default priority
protocol VINES with default priority
protocol IPX with default priority
protocol OSI with default priority
protocol VOFR with default priority
protocol AP2 with default priority
protocol ASRT with default priority

assigned tags:

default class is DEFAULT with priority NORMAL

BRS [i 2] Config>
```

Configuración de BRS y puesta en colas de prioridad

Ejemplo 2

```
BRS [i 1] [d1ci 17] Config>list

BANDWIDTH RESERVATION listing from SRAM
bandwidth reservation is enabled
maximum queue length 10, minimum queue length 3
total bandwidth allocated 60%
total classes defined (counting one local and one default) 3

class LOCAL has 10% bandwidth allocated
  protocols and filters cannot be assigned to this class.

class DEFAULT has 40% bandwidth allocated
  the following protocols and filters are assigned:
  protocol ASRT with priority NORMAL is not discard eligible
  filter NETBIOS with priority NORMAL is not discard eligible

class CLASS1 has 10% bandwidth allocated
  the following protocols and filters are assigned:
  protocol IP with priority NORMAL is not discard eligible
  protocol ARP with priority NORMAL is not discard eligible
  protocol DNA with priority NORMAL is not discard eligible
  protocol VINES with priority NORMAL is not discard eligible
  protocol IPX with priority NORMAL is discard eligible
  protocol OSI with priority NORMAL is not discard eligible
  protocol VOFR with priority NORMAL is not discard eligible
  protocol AP2 with priority NORMAL is not discard eligible
```

Ejemplo 3

```
BRS [i 1] [circuit defaults] Config>list

BANDWIDTH RESERVATION listing from SRAM
bandwidth reservation is enabled
interface number 1, default circuit
maximum queue length 10, minimum queue length 3
total bandwidth allocated 70%
total classes defined (counting one local and one default) 4

class LOCAL has 10% bandwidth allocated
  protocols and filters cannot be assigned to this class.

class DEFAULT has 40% bandwidth allocated
  the following protocols and filters are assigned:
  protocol DNA with default priority is not discard eligible
  protocol VINES with default priority is not discard eligible
  protocol IPX with default priority is not discard eligible
  protocol OSI with default priority is not discard eligible
  protocol VOFR with default priority is not discard eligible
  protocol AP2 with default priority is not discard eligible
  protocol ASRT with default priority is not discard eligible

class DEF1 has 10% bandwidth allocated
  protocol IP with priority NORMAL is not discard eligible.

class DEF2 has 10% bandwidth allocated
  protocol ARP with priority NORMAL is not discard eligible.

assigned tags:

default class is DEFAULT with priority NORMAL

BRS [i 1] [circuit defaults] Config>
```

Ejemplo 4

```
BRS Config>list
Bandwidth Reservation is available for 2 interfaces.
```

Interface	Type	State
1	FR	Enabled
2	PPP	Enabled

The use of HPR over IP port numbers is enabled.

Transmission Type	Port Number
XID exchange	12000
HPR network	12001
HPR high	12002
HPR medium	12003
HPR low	12004

Queue-length

Utilice el mandato **queue-length** para definir el número de paquetes que pueden ponerse en cada cola de prioridad BRS. Cada clase BRS tiene asignado un valor de prioridad para sus protocolos, filtros y códigos, y cada cola de prioridad puede almacenar el número de paquetes que se especifican con este mandato.

Sintaxis:

queue-length *longitud-máxima* *longitud-mínima*

Este mandato define el número máximo de almacenamientos intermedios que pueden ponerse en cada cola de prioridad BRS, así como el número máximo que pueden ponerse en cada cola de prioridad BRS cuando sean escasos los almacenamientos intermedios de entrada de direccionador.

Si emite **queue-length** para una interfaz PPP, el mandato define los valores de longitud de cola para cada cola de prioridad de cada clase-t BRS definida para la interfaz.

Si emite **queue-length** para una interfaz Frame Relay (en el indicador: BRS [i 0] Config>), el mandato define los valores de longitud de cola por omisión para cada cola de prioridad de cada clase-t BRS definida para cada circuito virtual permanente de la interfaz.

Si emite **queue-length** para un PVC Frame-Relay (en un indicador como éste: BRS [i 0] Config>), el mandato define los valores de longitud de cola para cada cola de prioridad de cada clase-t BRS definida para el PVC. Estos valores prevalecen sobre los valores de longitud de cola por omisión definidos para la interfaz Frame Relay.

Atención: No utilice este mandato a menos que sea esencial hacerlo. Los valores por omisión de la longitud de cola son los recomendados para la mayoría de usuarios. Si define unos valores demasiado elevados para la longitud de las colas, puede perjudicar gravemente al rendimiento del direccionador.

Set-circuit-defaults

Utilice el mandato **set-circuit-defaults** para acceder a los mandatos utilizados para establecer las definiciones de circuito por omisión para la gestión de clases de tráfico. Cualquier circuito Frame Relay en la interfaz que pueda utilizar utilizar las mismas clases de tráfico y asignaciones de protocolos, filtros y códigos, puede utilizar estas definiciones de circuito por omisión.

Sintaxis:

set-circuit-defaults

Show

Utilice el mandato **show** para visualizar las clases de ancho de banda definidas actualmente que están almacenadas en la RAM.

Sintaxis:

show *núm-interfaz*

Según el indicador en el que se emita el mandato **show**, se visualizarán varias salidas. Puede emitir el mandato **show** desde los indicadores siguientes:

- BRS [i x] Config> - indicador de nivel de interfaz para el número de interfaz x.
- BRS [i x] [dlci y] Config> - indicador de nivel de circuito para el circuito y en el número de interfaz Frame Relay x. El ejemplo siguiente muestra la salida del mandato show desde el indicador de nivel de circuito.

```
BRS [i 1] [dlci 17] Config>show
```

Protocol/Filter	Class	Priority	Discard Eligible
IP	CLASS1	NORMAL	NO
ARP	CLASS1	NORMAL	NO
DNA	CLASS1	NORMAL	NO
VINES	CLASS1	NORMAL	NO
IPX	CLASS1	NORMAL	YES
OSI	CLASS1	NORMAL	NO
VOFR	CLASS1	NORMAL	NO
AP2	CLASS1	NORMAL	NO
ASRT	DEFAULT	NORMAL	NO
NETBIOS	DEFAULT	NORMAL	NO

Se visualiza información sobre clases de tráfico en el indicador de interfaz para PPP y en el indicador de circuito para Frame Relay. Se visualiza información sobre clases de circuito en el indicador de interfaz Frame Relay.

Notas:

1. Cuando se utiliza este mandato en un indicador de circuito Frame Relay (BRS [i x] [dlci y] Config>), indica si el circuito utiliza definiciones de circuito por omisión o definiciones específicas de circuito para la gestión de clases de tráfico. Si el circuito utiliza definiciones de circuito por omisión, se visualizan las asignaciones de clases de tráfico, protocolos, filtros y códigos definidos actualmente para las definiciones de circuito por omisión. No obstante, si desea alterar las definiciones de circuito por omisión, tiene que dirigirse al indicador BRS[i x] [circuit defaults] Config> para efectuar los cambios.

2. Este mandato no se puede utilizar en el indicador BRS [i x] [circuit defaults] Config>.

Tag

Utilice el mandato **tag** para asignar un elemento de filtro MAC que se ha codificado durante la configuración de la característica de filtrado MAC al siguiente nombre de código BRS disponible. Los nombres de código BRS son TAG1, TAG2, TAG3, TAG4 y TAG5. Utilice el nombre de código BRS en el mandato assign para asignar el código a una clase de tráfico BRS.

Sintaxis:

tag *núm-código_filtro_mac*

Utilice el mandato **list** para listar cuáles son los códigos de filtro MAC que se han asignado a un nombre de código BRS y cuáles son los nombres de código BRS que se han asignado a una clase de tráfico de ancho de banda.

Nota: Si este mandato se utiliza para un circuito Frame Relay que utiliza actualmente definiciones de circuito por omisión para la gestión de clases de tráfico, se le preguntará si desea alterar temporalmente las definiciones de circuito por omisión. Si responde “Yes”, el circuito cambiará para utilizar definiciones específicas de circuito para la gestión de clases de tráfico y se permitirá el mandato. Si responde “No”, el mandato terminará anormalmente y se seguirán utilizando las definiciones de circuito por omisión para el circuito. Si desea modificar las definiciones de circuito por omisión, debe dirigirse al indicador de mandatos BRS [i x] [circuit defaults] Config>.

Untag

Utilice el mandato **untag** para eliminar la relación entre el número de código de filtro MAC y el nombre de código BRS. Sólo es posible eliminar un código si el nombre de código BRS correspondiente no se asigna a una clase de tráfico de ancho de banda.

Sintaxis:

untag *núm-código_filtro_mac*

Utilice el mandato **list** para mostrar cuáles son los códigos de filtro MAC que están asignados a un nombre de código BRS y cuáles son los nombres de código BRS que están asignados a una clase de tráfico.

Nota: Si este mandato se utiliza para un circuito Frame Relay que utiliza actualmente definiciones de circuito por omisión para la gestión de clases de tráfico, se le preguntará si desea alterar temporalmente las definiciones de circuito por omisión. Si responde “Yes”, el circuito cambiará para utilizar definiciones específicas de circuito para la gestión de clases de tráfico y se permitirá el mandato. Si responde “No”, el mandato terminará anormalmente y se seguirán utilizando las definiciones de circuito por omisión para el circuito. Si desea modificar las definiciones de circuito por omisión, debe dirigirse al indicador de mandatos BRS [i x] [circuit defaults] Config>.

Use-circuit-defaults

Utilice el mandato **use-circuit-defaults** en el nivel de circuito para suprimir las definiciones específicas de circuito y utilizar las definiciones de circuito por omisión para la gestión de clases de tráfico. Se le solicitará que confirme que desea utilizar los valores por omisión de circuito.

Sintaxis:

use-circuit-defaults

Notas:

1. Este mandato sólo se utiliza al configurar Frame Relay
2. Es preciso volver a cargar el direccionador para que los valores por omisión pasen a ser operativos.

Ejemplo:

```
BRS [i 1] [dlci 17] Config>use-circuit-defaults
This circuit is currently NOT using circuit defaults...
Are you sure you want to delete current definitions and use defaults ? (Yes or
[No]): y
Defaults are in effect for this circuit.
Please reload router for this command to take effect.
BRS [i 1] [dlci 17] Config>
```

Acceso al indicador de supervisión de la reserva de ancho de banda

Para acceder a los mandatos de supervisión de la reserva de ancho de banda y supervisar la reserva de ancho de banda en el direccionador, realice lo siguiente:

1. En el indicador OPCON (*), escriba **talk 5**.
2. En el indicador GWCON (+), escriba **feature brs**.
3. En el indicador BRS>, escriba **interface #**, donde # es el número de la interfaz que desea supervisar. Esta acción le conducirá al indicador de nivel de interfaz BRS, BRS [i x]>, donde x es el número de interfaz.

4. Sólo en el caso de Frame Relay, escriba **circuit #** en el indicador de interfaz para especificar el circuito en esta interfaz que desea supervisar.

Esta acción le conducirá al indicador de nivel de circuito BRS [i x] [dlci y]>, donde x es el número de interfaz e y es el número de circuito.

5. En el indicador, escriba el mandato de supervisión adecuado. (Consulte "Mandatos de supervisión de reserva de ancho de banda" en la página 51.)

El mandato **talk 5 (t 5)** permite acceder al proceso de supervisión.

El mandato **feature brs** permite acceder al proceso de supervisión BRS. Puede entrar este mandato utilizando el nombre (brs) o el número (1) de la característica.

El mandato **interface #** selecciona la interfaz específica que desea supervisar para la reserva de ancho de banda.

El mandato **circuit #** selecciona la DLCI de un circuito virtual permanente (PVC) Frame Relay.

Para regresar al indicador GWCON en cualquier momento, escriba el mandato **exit** en el indicador BRS>.

Una vez que haya accedido al indicador de supervisión de reserva de ancho de banda (BRS>), puede entrar en cualquiera de los mandatos específicos de supervisión, que se describen en la Tabla 5 en la página 51.

Mandatos de supervisión de reserva de ancho de banda

En esta sección se resumen y se explican los mandatos de supervisión de la Reserva de ancho de banda. La Tabla 5 muestra los mandatos de supervisión de la Reserva de ancho de banda. Los mandatos que pueden utilizarse difieren, según el indicador de supervisión de BRS (BRS>, BRS [i x]>, o BRS [i x] [dlci y]>).

Mandato	Utilizado sólo con FR	Función
? (Help)		Muestra todos los mandatos disponibles para este nivel de mandato o lista las opciones para mandatos específicos (si están a disposición). Consulte "Cómo obtener ayuda" en la página xxxiv
Circuit	sí	Selecciona la DLCI de un circuito virtual permanente (PVC) Frame Relay. Para supervisar el tráfico de reserva de ancho de banda Frame Relay, debe encontrarse en el nivel de indicador de circuito.
Clear		Borra los contadores de clase-t actuales y los almacena como los últimos contadores de clase-t. Los contadores se listan según la clase.
Clear-circuit-class	sí	Borra los contadores de clase-c actuales y los almacena como los últimos contadores de clase-c. Los contadores se listan según la clase.
Counters		Visualiza los contadores de clase-t actuales.
Counters-circuit-class	sí	Visualiza los contadores de clase-c actuales.
Interface		Selecciona la interfaz que se va a supervisar. Nota: Es preciso entrar este mandato antes de utilizar otros mandatos de supervisión de reserva de ancho de banda.
Last		Visualiza los últimos contadores de clase-t que se han guardado.
Last-circuit-class	sí	Visualiza los últimos contadores de clase-c que se han guardado.
Exit		Le devuelve al nivel de mandatos anterior. Consulte "Cómo salir de un entorno de nivel inferior" en la página xxxiv

Circuit

Nota: Sólo se utiliza al supervisar Frame Relay.

Utilice el mandato **circuit** para seleccionar la DLCI de un PVC Frame Relay PVC para su supervisión. Este mandato sólo puede emitirse desde el indicador de supervisión de interfaz BRS (BRS [i #]>).

Sintaxis:

circuit *núm-circuito-virtual-permanente*

Después de haber seleccionado el circuito Frame Relay, pueden utilizarse los siguientes mandatos en el indicador de circuito:

```
CLEAR  
COUNTERS  
LAST  
EXIT
```

Clear

Utilice el mandato **clear** para guardar los contadores actuales de clase-t de reserva de ancho de banda, para que puedan recuperarse mediante el mandato **last** y se puedan borrar los valores. Los contadores se conservan según la clase de tráfico de ancho de banda.

Sintaxis:

clear

Clear-Circuit-Class

Nota: Sólo se utiliza al supervisar Frame Relay.

Utilice el mandato **clear-circuit-class** para guardar los contadores actuales de clase-c de reserva de ancho de banda, para que puedan recuperarse mediante el mandato **last-circuit-class** y se puedan borrar los valores. Los contadores se conservan según la clase de circuito.

Sintaxis:

clear-circuit-class

Counters

Utilice el mandato **counters** para visualizar las estadísticas que describen el tráfico de reserva de ancho de banda para las clases de tráfico configuradas para una interfaz PPP o un circuito Frame Relay.

Sintaxis:

counters

Ejemplo: counters


```

Bandwidth Reservation Counters
interface number 1
Class          Pkt Xmit    Bytes Xmit    Bytes Ovfl    Pkt Ovfl    Q_len
LOCAL          10          914           0              0            0
  LOW          0           0             0              0            0
  NORMAL       10          914           0              0            0
  HIGH         0           0             0              0            0
  URGENT       0           0             0              0            0
DEFAULT        55          5555          0              0            0
  LOW          0           0             0              0            0
  NORMAL       20          5020          0              0            0
  HIGH         0           0             0              0            0
  URGENT       35          535           0              0            0
CLASS_1        5           910           0              0            0
  LOW          0           0             0              0            0
  NORMAL       5           910           0              0            0
  HIGH         0           0             0              0            0
  URGENT       0           0             0              0            0
CLASS_2        70          4123          0              0            0
  LOW          10          617           0              0            0
  NORMAL       55          3117          0              0            0
  HIGH         0           0             0              0            0
  URGENT       5           389           0              0            0
TOTAL          140         11502         0              0

```

Bytes Ovfl

Lista el número de bytes de los paquetes que no se han podido transmitir porque se ha alcanzado la longitud máxima de cola para una cola de prioridad, o porque el paquete no se ha podido poner en cola, ya que la cola de prioridad estaba en el umbral mínimo de longitud de cola y el paquete procedía de una interfaz que disponía de pocos almacenamientos intermedios de recepción.

Pkt Ovfl Lista el número de paquetes que no se han podido transmitir porque se ha alcanzado la longitud máxima de cola para una cola de prioridad, o porque el paquete no se ha podido poner en cola, ya que la cola de prioridad estaba en el umbral mínimo de longitud de cola y el paquete procedía de una interfaz que disponía de pocos almacenamientos intermedios de recepción.

Q_len Número actual de paquetes que esperan la transmisión de cada una de las colas de prioridad en cada clase de tráfico.

Counters-circuit-class

Nota: Sólo se utiliza al supervisar Frame Relay.

Utilice el mandato **counters-circuit-class** para visualizar las estadísticas de las clases de tráfico configuradas para un circuito Frame Relay.

Sintaxis:

counters-circuit-class

Ejemplo: counters-circuit-class

```

Bandwidth Reservation Circuit Class Counters
Interface 1

Class          Pkt Xmit    Bytes Xmit    Bytes Ovfl
DEFAULT        25          3402          26
CIRCLASS1      1           56            0
CIRCLASS2      0           0             0
TOTAL          26          3458          26

```

Interface

Utilice el mandato **interface** para seleccionar la interfaz serie a la que se aplicarán los mandatos de supervisión de reserva de ancho de banda. *La reserva de ancho de banda está soportada en los direccionadores que ejecutan las interfaces PPP (Protocolo punto a punto) y Frame Relay.*

Sintaxis:

interface *núm-interfaz*

Nota: Para entrar mandatos de reserva de ancho de banda para una interfaz nueva, es preciso entrar este mandato antes de utilizar ningún otro mandato de supervisión de reserva de ancho de banda. Si ha salido del indicador de supervisión de reserva de ancho de banda (BRS>) y desea volver a supervisar la reserva de ancho de banda, en primer lugar debe entrar este mandato de nuevo.

Para supervisar la Reserva de ancho de banda en una interfaz determinada, en el indicador de supervisión BRS>, escriba el número de la interfaz. A continuación, puede utilizar los mandatos de supervisión de la reserva de ancho de banda tal como se describen en este capítulo.

Last

Utilice el mandato **last** para visualizar las últimas estadísticas de clase-t que se han guardado. Las estadísticas de clase-t se visualizan con el mismo formato que para el mandato **counters**.

Sintaxis:

last

Last-circuit-class

Nota: Sólo se utiliza al supervisar Frame Relay.

Utilice el mandato **last-circuit-class** para visualizar las últimas estadísticas de clase de circuito que se han guardado. Las estadísticas de clase-c se visualizan con el mismo formato que para el mandato **counters-circuit-class**.

Sintaxis:

last-circuit-class

Utilización del filtrado MAC

Este capítulo describe cómo utilizar el control de acceso a medio (MAC) para especificar que se apliquen filtros de paquetes a los paquetes durante el proceso. Incluye las secciones siguientes:

- “Filtrado MAC y tráfico DLSw”
- “Parámetros de filtrado MAC” en la página 56

Los filtros son un conjunto de reglas aplicadas a un paquete para determinar cómo debe gestionarse el paquete durante la operación de puente. El filtrado MAC sólo afecta al tráfico con puente.

Nota: El Filtrado MAC está permitido en el tráfico de túnel.

Durante el proceso de filtrado, los paquetes se procesan, filtran o codifican durante el proceso de puente. Las acciones son:

- **Procesado** – Se permite que los paquetes pasen a través del puente sin verse afectados.
- **Filtrado/ph>** – **No se permite que los paquetes pasen a través del puente.**
- **Codificado** – Se permite que los paquetes pasen a través del puente, pero se marcan con un número entre el rango de 1 a 64, basándose en un parámetro configurable.

Un filtro MAC se compone de los tres objetos siguientes:

1. Elemento de filtro – una sola regla que se aplica al campo de dirección o a una ventana de datos arbitraria en un paquete. El resultado de aplicar la regla es una condición verdadera (coincidencia satisfactoria) o falsa (sin coincidencia).
2. Lista de filtros – contiene una lista de uno o más elementos de filtro.
3. Filtro – contiene un conjunto de listas de filtros.

Filtrado MAC y tráfico DLSw

Puede filtrar el tráfico LLC entrante para la red DLSw implementando el Filtrado MAC.

Para configurar un filtro para LLC, utilice el número de *Red de puente* como número de interfaz para el filtro. Determine el número de Red de puente añadiendo dos al número de interfaces configurado para el direccionador. Entre el mandato **list devices** en el indicador `Config>`, o bien entre **configuration** en el indicador `+` para ver una lista de interfaces.

En el ejemplo siguiente, el número de Red de puente es 7.

Ifc 0 Token Ring	Slot: 1	Port: 1
Ifc 1 Token Ring	Slot: 1	Port: 2
Ifc 2 Token Ring	Slot: 2	Port: 1
Ifc 3 Token Ring	Slot: 2	Port: 2
Ifc 4 Ethernet	Slot: 4	Port: 1
Ifc 5 Ethernet	Slot: 4	Port: 2

Por ejemplo, cuando se configura un filtro para la Red de puente, el direccionador no elimina las tramas que coinciden con filtros exclusivos. En lugar de ello, reenvía las tramas al puente.

Parámetros de filtrado MAC

Puede especificar algunos de los parámetros siguientes, o todos ellos, para crear un filtro:

- Dirección MAC de origen o de destino
- Datos que deben emparejarse en el paquete
- Máscara que debe aplicarse a los filtros del paquete que se va a filtrar
- Número de interfaz
- Designación de entrada/salida
- Designación de incluir/excluir/codificar
- Valor del código (si se proporciona designación de codificar)

Parámetros de los elementos de filtro

Se utilizan los parámetros siguientes para construir un elemento de filtro de direcciones:

- Tipo de dirección: SOURCE o DESTINATION
- Código: un *valor de código*
- Máscara de dirección: una *máscara hexadecimal*

Cada elemento de filtro especifica que un tipo de dirección (SOURCE o DESTINATION) se empareje con el tipo del paquete.

La máscara de dirección es una serie de números entrados en formato hexadecimal, que se utilizan comparando las direcciones del paquete. La máscara se aplica a la dirección MAC SOURCE o DESTINATION del paquete antes de compararlo con la dirección MAC especificada.

La máscara de dirección debe tener la misma longitud que la dirección MAC y especifica los bytes a los que se aplica la operación AND lógica con los bytes de la dirección MAC, antes de realizar la comparación de igualdad con la dirección MAC especificada. Si no se especifica ninguna máscara, se supone que todas son 1.

Parámetros de lista de filtros

Se utilizan los parámetros siguientes para construir una lista de filtros:

- Nombre: una *serie ASCII*
- Lista de elementos de filtro: *elemento de filtro 1 . . . elemento de filtro n*
- Acción: INCLUDE, EXCLUDE, TAG(*n*)

Una lista de filtros se construye a partir de uno o más elementos de filtro. A cada lista de filtros se le da un nombre exclusivo.

La aplicación de una lista de filtros a un paquete consiste en comparar cada elemento de filtro en el orden en que se han añadido los elementos de filtro a la lista. Si cualquier elemento de filtro de la lista devuelve una condición TRUE, la lista de filtros devolverá su acción designada.

Parámetros de filtro

Los parámetros siguientes se utilizan para construir un filtro:

- Nombres de listas de filtros: *serie ASCII 1 . . . serie ASCII n*
- Número de interfaz: un *número de IFC*
- Dirección de puerto: INPUT o OUTPUT
- Acción por omisión: INCLUDE, EXCLUDE o TAG
- Código por omisión: un *valor de código*

Un filtro se construye asociando un grupo de nombres de listas de filtros a un número de interfaz y asignándole una designación INPUT o OUTPUT. La aplicación de un filtro a un paquete quiere decir que cada una de las listas de filtros asociadas debe aplicarse a los paquetes que se reciben (INPUT) o se envían (OUTPUT) en la interfaz con el número especificado.

Cuando un filtro evalúa un paquete a una condición INCLUDE, se reenvía el paquete. Cuando un filtro evalúa un paquete a una condición EXCLUDE, se elimina el paquete. Cuando un filtro evalúa a una condición TAG, el paquete en cuestión se reenvía con un código.

La acción por omisión, que es el resultado de una falta de emparejamiento para todas sus listas de filtros, es un parámetro adicional de cada filtro. Esta acción por omisión es INCLUDE. Puede definirse como INCLUDE, EXCLUDE o TAG. Además, si la acción por omisión es TAG, también se proporciona un valor de código.

Utilización de los códigos del filtrado MAC

La lista siguiente incluye algunos usos para los códigos de filtrado MAC

- El filtrado de direcciones MAC lo gestionan conjuntamente la reserva de ancho de banda y la característica Filtrado MAC (MCF) utilizando códigos. Un usuario con reserva de ancho de banda puede establecer categorías en el tráfico de puente, por ejemplo asignándole un código.
- El proceso de codificación se realiza creando un elemento de filtro en la consola de configuración de filtrado MAC y, después, asignándole un código. Este código se utiliza para configurar una clase de ancho de banda para todos los paquetes asociados a este código. Los valores del código deben estar en el rango de 1 a 64.
- Una vez que haya creado un filtro codificado en el proceso de configuración de filtrado MAC, se utiliza el mandato de configuración **tag** de BRS (Reserva de ancho de banda) para asignar un nombre de código BRS (TAG1, TAG2, TAG3, TAG4 o TAG5) al número de código de filtro MAC. A continuación, utilice el nombre de código BRS en el mandato **assign** de BRS para asignar el filtro MAC correspondiente a una clase de tráfico y prioridad de ancho de banda.
- Pueden definirse 5 direcciones MAC codificadas como máximo, de 1 a 5. Primero se busca TAG1, después TAG2, y así sucesivamente hasta TAG5.

Los códigos también pueden referirse a “grupos” en IP Tunnel. Los extremos de IP Tunnel pueden pertenecer a cualquier número de grupos, con paquetes asignados a un grupo determinado a través de la característica de codificación del filtrado de direcciones MAC.

Utilización del filtrado MAC

Configuración y supervisión del filtrado MAC

Este capítulo describe cómo acceder a los indicadores de configuración y supervisión del Filtrado MAC y cómo utilizar los mandatos disponibles. Incluye las secciones siguientes:

- “Acceso al indicador de supervisión de filtrado MAC” en la página 67
- “Mandatos de supervisión de filtrado MAC” en la página 67

Acceso al indicador de configuración de filtrado MAC

Utilice el mandato **feature** del proceso CONFIG para acceder a los mandatos de configuración del filtrado MAC. El mandato **feature** permite acceder a los mandatos de configuración para características específicas fuera de los procesos de configuración de interfaz de red y protocolos.

Entre un signo de cierre de interrogación después del mandato **feature** para obtener una lista de las características disponibles para su release del software. Por ejemplo:

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

Para acceder al indicador de configuración del filtrado MAC, entre el mandato **feature** seguido del *número de característica* (3) o *nombre corto* (MCF). Por ejemplo:

```
Config> feature mcf
MAC Filtering user configuration
Filter config>
```

Una vez que haya accedido al indicador de configuración de filtrado MAC, puede empezar a entrar mandatos de configuración específicos. Para regresar al indicador CONFIG en cualquier momento, entre el mandato **exit** en el indicador de configuración del filtrado MAC.

Mandatos de configuración del filtrado MAC

En esta sección se resumen los mandatos de configuración del filtrado MAC. Entre estos mandatos en el indicador `Filter config>`.

Utilice los mandatos siguientes para configurar la característica de filtrado MAC.

Tabla 6 (Página 1 de 2). Resumen de los mandatos de configuración del filtrado MAC

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxiv.
Attach	Añade una lista de filtros a un filtro.
Create	Crea una lista de filtros o un filtro INPUT u OUTPUT.

Configuración de filtrado MAC

Tabla 6 (Página 2 de 2). Resumen de los mandatos de configuración del filtrado MAC

Mandato	Función
Default	Define la acción por omisión para el filtro especificado como EXCLUDE, INCLUDE o TAG.
Delete	Elimina toda la información asociada a una lista de filtros. También suprime un filtro creado mediante el mandato create filter.
Detach	Elimina una lista de filtros de un filtro.
Disable	Inhabilita el Filtrado MAC por completo o inhabilita un filtro determinado.
Enable	Habilita el Filtrado MAC por completo o habilita un filtro determinado.
List	Lista un resumen de todas las listas de filtros y los filtros configurados por el usuario. También genera una lista de listas de filtros conectadas para este filtro y toda la información subsiguiente para el filtro.
Move	Reordena las listas de filtros conectadas a un filtro específico.
Reinit	Vuelve a inicializar todo el sistema de Filtrado MAC a partir de una configuración actualizada, sin que ello afecte al resto del direccionador.
Set-Cache	Cambia el tamaño de la antememoria para un filtro.
Update	Añade o suprime información de una lista de filtros específica. Le conducirá a un menú con los submandatos adecuados.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiv.

Attach

Utilice el mandato **attach** para añadir una lista de filtros a un filtro.

Un filtro se construye asociando un grupo de nombres de listas de filtros a un número de interfaz. Una lista de filtros se construye a partir de uno o más elementos de filtro.

Sintaxis:

attach *nombre-lista-filtros número-filtro*

Create

Utilice el mandato **create** para crear una lista de filtros o un filtro INPUT u OUTPUT.

Sintaxis:

create *list nombre-lista-filtros*
filter [input u output] número-interfaz

list *nombre-lista-filtros*

Crea una lista de filtros. Las listas reciben nombres que son series exclusivas (*nombre-lista-filtros*) a elección del usuario y de 16 caracteres como máximo. Este nombre se utiliza para identificar una lista de filtros que se esté construyendo. Este nombre se utiliza también con otros mandatos asociados a la lista de filtros.

filter [input u output] número-interfaz

Crea un filtro y lo coloca en la red asociada a la dirección de INPUT u OUTPUT en la interfaz proporcionada por un número de interfaz. Por

omisión, este filtro se crea sin listas de filtros conectadas, tiene la acción por omisión INCLUDE y tiene el valor ENABLED (habilitado).

Default

Utilice el mandato **default** para definir la acción por omisión para el filtro con un número de filtro especificado para excluir, incluir o codificar.

Sintaxis:

```
default          exclude número-filtro
                  include número-filtro
                  tag número-código número-filtro
```

exclude *número-filtro*

Define la acción por omisión para el filtro con un número de filtro específico para excluir.

include *número-filtro*

Define la acción por omisión para el filtro con un número de filtro específico para incluir.

tag *número-código número-filtro*

Define la acción por omisión para el filtro con un número de filtro específico para TAG y define el valor de código asociado al número de código.

Delete

Utilice el mandato **delete** para eliminar toda la información asociada a una lista de filtros y para liberar una serie asignada como nombre para una lista de filtros nueva. Si la lista de filtros está conectada a un filtro que el usuario ya ha creado, este mandato no suprimirá nada y aparecerá un mensaje de error en la consola. Además, se borrarán también todos los elementos de filtro que pertenezcan a esta lista.

Este mandato suprime también un filtro creado utilizando el mandato **create filter**.

Sintaxis:

```
delete          list lista-filtros
                  filter número-filtro
```

list *lista-filtros*

Elimina toda la información asociada a una lista de filtros y libera una serie no asignada como nombre para una lista de filtros nueva. La lista de filtros debe ser una serie entrada mediante un mandato **create list** anterior.

Si la lista de filtros está conectada a un filtro que el usuario ya ha creado, este mandato no suprimirá nada y aparecerá un mensaje de error en la consola. Además, cuando se utilice este mandato se borrarán también todos los elementos de filtro que pertenezcan a esta lista.

filter *número-filtro*

Suprime un filtro creado utilizando el mandato **create filter**.

Detach

Utilice el mandato **detach** para suprimir un nombre de lista de filtros (parámetro lista-filtros) de un filtro (parámetro número-filtro).

Sintaxis:

detach *nombre-lista-filtros número-filtro*

Disable

Utilice el mandato **disable** para inhabilitar el Filtrado MAC por completo o para inhabilitar un filtro determinado.

Sintaxis:

disable all
 filter *número-filtro*

all Inhabilita el Filtrado MAC por completo. No obstante, los filtros siguen estando definidos como ENABLED si se habilitaron previamente.

filter *número-filtro*
 Inhabilita un filtro específico. El parámetro número-filtro corresponde a los números visualizados en el mandato **list filters**.

Enable

Utilice el mandato **enable** para habilitar el Filtrado MAC por completo o habilitar un filtro determinado.

Sintaxis:

enable all
 filter *número-filtro*

all Habilita el Filtrado MAC por completo, aunque los propios filtros pueden definirse como DISABLED.

filter *número-filtro*
 Habilita un filtro específico. El parámetro número-filtro corresponde a los números visualizados en el mandato **list filters**.

List

Utilice el mandato **list** para listar un resumen de todas las listas de filtros y los filtros configurados por el usuario. No se proporciona ninguna lista de todas las listas de filtros conectadas a un filtro. Otra información visualizada es la siguiente:

- Una lista que contiene el estado del sistema de filtrado (ENABLE, DISABLE)
- El conjunto de registros de lista de filtros configurados.
- Cada uno de los registros de filtro configurados.

Además, se visualiza la siguiente información para cada filtro:

- Número de filtro
- Número de interfaz
- Dirección del filtro (INPUT, OUTPUT)
- Estado del filtro (ENABLE, DISABLE)
- Acción del filtro por omisión (TAG, INCLUDE, EXCLUDE).

Este mandato genera también una lista de listas de filtros conectadas para este filtro y toda la información subsiguiente para el filtro.

Sintaxis:

list all
 filter *número-filtro*

all Muestra un resumen de todas las listas de filtros y los filtros configurados.

filter *número-filtro*

Genera una lista de listas de filtros conectadas para el filtro especificado y toda la información subsiguiente para el filtro.

Move

Utilice el mandato **move** para reordenar las listas de filtros conectadas a un filtro especificado (proporcionado por el parámetro *número-filtro*). La lista proporcionada por *Nombre1-lista-filtros* se coloca inmediatamente antes que la lista proporcionada por *Nombre2-lista-filtros*.

Sintaxis:

move *nombre1-lista-filtros nombre2-lista-filtros número-filtro*

Reinit

Utilice el mandato **reinit** para volver a inicializar todo el sistema de Filtrado MAC desde una configuración actualizada, sin que ello afecte al resto del direccionador.

Sintaxis:

reinit

Set-Cache

Utilice el mandato **set-cache** para cambiar el tamaño de antememoria por omisión (16) por un número en el rango de 4 a 32768.

Sintaxis:

set-cache *tamaño-antememoria número-filtro*

Update

Utilice el mandato **update** para añadir o suprimir información en una lista de filtros específica. La utilización de este mandato con el nombre-lista-filtros que se desea le conducirá al indicador `Filter nombre-lista-filtros Config>` para esa lista de filtros específica. Desde este nuevo indicador, puede modificar la información en la lista especificada.

El nuevo nivel de indicador se utiliza para añadir o suprimir elementos de lista de las listas de filtros. El orden en que se especifican los elementos de filtro para una lista de filtros dada es importante, ya que determina el orden en que se aplicarán los elementos de filtro a un paquete.

Sintaxis:

update *nombre-lista-filtros*

Submandatos de actualización

En esta sección se resumen los submandatos de configuración del filtrado MAC. Entre estos submandatos en el indicador `Filter nombre-lista-filtros config>`.

Tabla 7. Resumen de los submandatos de actualización

Submandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxiv.
Add	Añade filtros de direcciones MAC de origen o destino, o un filtro de ventana. También añade elementos de filtro a una lista de filtros.
Delete	Elimina elementos de filtro de una lista de filtros.
List	Lista un resumen de todas las listas de filtros y los filtros que el usuario ha configurado. También genera una lista de listas de filtros conectadas para este filtro y toda la información subsiguiente para el filtro.
Move	Reordena las listas de filtros conectadas a un filtro especificado.
Set-Action	Define un elemento de filtro para evaluar la condición INCLUDE, EXCLUDE o TAG (con una opción de número de código).
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiv.

Utilice los submandatos siguientes para actualizar una lista de filtros.

Add

Utilice el submandato **add** para añadir elementos de filtro a una lista de filtros. Específicamente, este submandato permite añadir un número hexadecimal para compararlo con la dirección MAC de origen o de destino, o una secuencia de datos de ventana con máscara para compararla con un paquete de datos.

El orden en que se añaden los elementos de filtro a una lista de filtros determinada es importante, porque determina el orden en que se aplican los elementos de filtro a un paquete.

Cada utilización del submandato **add** crea un elemento de filtro en la lista de filtros. Al primer elemento de filtro creado se le asigna el número de elemento de filtro 1, al siguiente se le asigna el número 2, y así sucesivamente. Después de entrar un submandato **add** de manera satisfactoria, el direccionador mostrará el número del elemento de filtro que se acaba de añadir.

Cuando se produce la primera coincidencia, se detiene la aplicación de elementos de filtro y la lista de filtros evalúa como INCLUDE, EXCLUDE o TAG, según la acción designada de la lista de filtros. Si no se produce ninguna coincidencia en ninguno de los elementos de filtro de una lista de filtros, se devuelve la acción por omisión (INCLUDE, EXCLUDE o TAG) del filtro.

Sintaxis: `add` *source dir-MAC-hex máscara-hex*
destination dir-MAC-hex máscara-hex
window MAC valor-desplazamiento datos-hex
máscara-hex

*window INFO valor-desplazamiento datos-hex
máscara-hex*

source *dir-MAC-hex máscara-hex*

Añade un número hexadecimal para compararlo con la dirección MAC de origen. **dir-MAC-hex** debe ser un número par de dígitos hexadecimales, con un máximo de 16 dígitos, y se debe entrar sin que haya un 0x delante.

El parámetro máscara-hex debe tener la misma longitud que dirección-MAC-hex y se le aplica la operación AND lógica con la dirección MAC designada del paquete. El argumento de máscara-hex por omisión debe ser todo 1 de formato binario.

El parámetro dir-MAC-hex se puede especificar en orden de bits canónico o no canónico. Un orden de bits canónico se especifica como un simple número hexadecimal (por ejemplo, 000003001234). También se puede representar como una serie de dígitos hexadecimales con un guión (-) entre cada dos dígitos (por ejemplo, 00-00-03-00-12-34).

Un orden de bits no canónico se especifica como una serie de dígitos hexadecimales con un signo de dos puntos (:) entre cada dos dígitos (por ejemplo, 00:00:C9:09:66:49). Las direcciones MAC de elementos de filtro se visualizarán siempre mediante un guión (-) o dos puntos (:) para distinguir entre las representaciones canónicas y no canónicas.

destination *dir-MAC-hex máscara-hex*

Actúa de forma idéntica al submandato **add source**, salvo que el emparejamiento se realiza con la dirección MAC de destino del paquete, no la de origen.

window MAC *valor-desplazamiento datos-hex máscara-hex*

Añade un elemento de filtro de ventana deslizante mediante el desplazamiento especificado (calculado desde el inicio de la trama) que empareja los datos hexadecimales, con la máscara, con los datos de paquete.

window INFO *valor-desplazamiento datos-hex máscara-hex*

Esto es similar al mandato **add window mac**, salvo que el desplazamiento se calcula respecto al principio del campo de información.

Delete

Utilice el submandato **delete** para eliminar elementos de filtro de una lista de filtros. Suprime elementos de filtro especificando el número de elemento de filtro que se asignó al elemento al añadirlo.

Cuando se utiliza el submandato **delete**, se rellena cualquier hueco existente en la secuencia numérica. Por ejemplo, si existen los elementos de filtro 1, 2, 3 y 4 y se suprime el elemento de filtro 3, el elemento de filtro 4 se vuelve a numerar como 3.

Sintaxis:

delete *número-elemento-filtro*

List

Utilice el submandato **list** para imprimir un listado de todos los registros de elementos de filtro. Se visualiza la siguiente información acerca de cada elemento de filtro Dirección-MAC:

- dirección MAC y máscara de dirección en formato canónico o no canónico.
- números de elementos de filtro
- tipo de dirección (de origen o destino)
- acción de lista de filtros

Sintaxis:

```
list                canonical
                    noncanonical
                    mac-address canonical
                    mac-address noncanonical
                    window
```

canonical

Imprime un listado de todos los registros de elemento de filtro en una lista de filtros, proporcionando los números de elemento, el tipo de dirección (SRC, DST), la dirección MAC en formato canónico y la máscara de dirección en formato canónico. También se da la acción de la lista de filtros.

mac-address canonical

Imprime un listado de todos los registros de elemento de filtro en una lista de filtros, proporcionando los números de elemento, el tipo de dirección (SRC, DST), la dirección MAC en formato canónico y la máscara de dirección en formato canónico. Además, se da la acción de la lista de filtros.

noncanonical

Imprime un listado de todos los registros de elemento de filtro en una lista de filtros, proporcionando los números de elemento, el tipo de dirección (SRC, DST), la dirección MAC en formato no canónico y la máscara de dirección en formato no canónico. También se da la acción de la lista de filtros.

mac-address noncanonical

Imprime un listado de todos los registros de elemento de filtro en una lista de filtros, proporcionando los números de elemento, el tipo de dirección (SRC, DST), la dirección MAC en formato no canónico y la máscara de dirección en formato no canónico. También se da la acción de la lista de filtros.

window

Imprime un listado de todos los registros de elemento de filtro de ventana deslizante en una lista de filtros, proporcionando los números de elemento, la base, el desplazamiento, los datos y la máscara. También se da la acción de la lista de filtros.

Move

El submandato **move** reordena los elementos de filtro en la lista de filtros. El elemento de filtro cuyo número se especifica mediante *nombre1-elemento-filtro* se mueve y se vuelve a numerar justo antes de *nombre2-elemento-filtro*.

Sintaxis:

move *nombre1-elemento-filtro nombre2-elemento-filtro*

Set-Action

El submandato **set-action** permite definir un elemento de filtro para evaluar la condición INCLUDE, EXCLUDE o TAG (con una opción de número de código). Si uno de los elementos de filtro de la lista de filtros coincide con el contenido del paquete examinado para el filtrado, la lista de filtros evaluará con la condición especificada. El valor por omisión es INCLUDE.

Sintaxis:

set-action [INCLUDE, EXCLUDE o TAG] *número-código*

Acceso al indicador de supervisión de filtrado MAC

Utilice el mandato **feature** del proceso GWCON para acceder a los mandatos de supervisión del filtrado MAC. El mandato **feature** permite acceder a los mandatos de supervisión para características específicas del direccionador fuera de los procesos de supervisión de interfaz de red y protocolos.

Entre un signo de cierre de interrogación después del mandato **feature** para obtener una lista de las características disponibles para su versión del software. Por ejemplo:

```
+ feature ?
WRS
BRS
MCF
```

Para acceder al indicador de supervisión de filtrado MAC, entre el mandato **feature** seguido del número de característica (3) o del nombre corto (MCF). Por ejemplo:

```
+ feature mcf
MAC Filtering user monitoring
Filter>
```

Una vez que haya accedido al indicador de supervisión de filtrado MAC, puede empezar a entrar mandatos de supervisión específicos. Para regresar al indicador GWCON en cualquier momento, entre el mandato **exit** en el indicador de supervisión del filtrado MAC.

Mandatos de supervisión de filtrado MAC

En esta sección se resumen los mandatos de supervisión del filtrado MAC. Entre estos mandatos en el indicador Filter>.

Configuración de filtrado MAC

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado "Cómo obtener ayuda" en la página xxxiv.
Clear	Borra las estadísticas "por filtro" listadas con el mandato list filter.
Disable	Inhabilita globalmente el Filtrado MAC o sólo "por cada filtro".
Enable	Habilita globalmente el Filtrado MAC o sólo "por cada filtro".
List	Lista un resumen de las estadísticas y los valores para cada filtro que se ejecuta actualmente en el direccionador.
Reinit	Vuelve a inicializar todo el sistema de Filtrado MAC a partir de una configuración actualizada, sin que ello afecte al resto del direccionador.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página xxxiv.

Utilice los mandatos siguientes para supervisar la característica de filtrado MAC.

Clear

Utilice el mandato **clear** para borrar las estadísticas del filtro.

Sintaxis:

clear all
 filter *número-filtro*

all Borra las estadísticas listadas por el mandato **list all**.

filter *número-filtro*
 Borra las estadísticas listadas por el mandato **list filter**.

Disable

Utilice el mandato **disable** para inhabilitar globalmente el filtrado MAC. Este mandato no inhabilita cada filtro individualmente.

El mandato inhabilita también un filtro, como especifica el número de filtro. Este filtro se inhabilita sin modificar los registros de configuración. Si no se proporciona ningún argumento, el filtrado MAC se inhabilita globalmente.

Sintaxis:

disable all
 filter *número-filtro*

all Inhabilita globalmente el filtrado MAC. Este mandato no inhabilita cada filtro individualmente.

filter *número-filtro*
 Inhabilita el filtro especificado por el número de filtro. Este filtro se inhabilita sin modificar los registros de configuración. Si no se proporciona ningún número de filtro, el filtrado MAC se inhabilita globalmente.

Enable

Utilice el mandato **enable** para habilitar globalmente el filtrado MAC. Este mandato no habilita cada filtro individualmente.

El mandato habilita también un filtro, como especifica el número de filtro. Este filtro se habilita sin modificar los registros de configuración. Si no se proporciona ningún argumento, el filtrado MAC se habilita globalmente.

Sintaxis:

```
enable          all
                  filter número-filtro
```

all Habilita globalmente el filtrado MAC. Este mandato no habilita cada filtro individualmente.

filter *número-filtro*

Habilita el filtro especificado por el número de filtro. Este filtro se habilita sin modificar los registros de configuración. Si no se proporciona ningún número de filtro, el filtrado MAC se habilita globalmente.

List

Utilice el mandato **list** para listar un resumen de las estadísticas y los valores para cada filtro que se ejecuta actualmente en el direccionador. Se visualiza la siguiente información para cada filtro cuando se utiliza el mandato **list all**:

- Acción por omisión
- Tamaño de antememoria
- Código por omisión
- Estado (habilitado/inhabilitado)
- Número de paquetes que se han filtrado como INCLUDE, EXCLUDE o TAG.

Además, el mandato **list filter** visualiza la siguiente información para un filtro específico:

- Toda la información visualizada por el mandato list all
- Todas las listas de filtros que se ejecutan actualmente en este filtro, incluidas las siguientes:
 - Lista nombre
 - Lista acción
 - Lista código
 - Número de paquetes que cada lista de filtros ha filtrado.

Sintaxis:

```
list           all
                  filter número-filtro
```

all Lista las estadísticas y los valores para cada filtro que se ejecuta actualmente en el direccionador.

filter *número-filtro*

Genera estadísticas y valores para cada filtro, más todas las listas de filtros que se ejecutan actualmente en este filtro.

Reinit

Utilice el mandato **reinit** para volver a inicializar todo el sistema de Filtrado MAC desde una configuración actualizada, sin que ello afecte al resto del direccionador.

Sintaxis:

`reinit`

Utilización de Restauración de WAN

Este capítulo incluye las secciones siguientes:

- “Visión general de Restauración de WAN, Redireccionamiento de WAN y Marcación en desbordamiento”
- “Antes de empezar” en la página 73
- “Procedimiento de configuración para la Restauración de WAN” en la página 74
- “Configuración de circuito de marcación secundario” en la página 74

Visión general de Restauración de WAN, Redireccionamiento de WAN y Marcación en desbordamiento

Las características Restauración de WAN, Redireccionamiento de WAN y Marcación en desbordamiento, tienen funciones similares y podrían confundirse. Esta visión general debería ayudarle a decidir cuál de estas funciones será útil para el usuario y le ayudará a encontrar la información que necesita para configurarlas.

Los mandatos de configuración para las tres características están incluidos en el capítulo "Configuración de Restauración de WAN". Para obtener información adicional acerca Redireccionamiento de WAN y Marcación en desbordamiento, consulte “La característica Redireccionamiento de WAN” en la página 99.

Restauración de WAN

Restauración de WAN es la función más básica de todas. Al utilizar la Restauración de WAN, configura un enlace primario y otro secundario. En caso de que el enlace primario falle, se inicia el enlace secundario y asume las características del primario. No configure ninguna definición de protocolo en el enlace secundario, porque utiliza las definiciones de protocolo del enlace primario.

Para la Restauración de WAN:

- Existe un emparejamiento entre un enlace primario y otro secundario.
- Sólo puede configurar un enlace primario para utilizar un enlace secundario específico.
- No configure definiciones de protocolo (por ejemplo: direcciones de protocolo) en el enlace secundario.
- El enlace primario puede ser una interfaz serie PPP o un interfaz PPP multienlace. No puede ser una interfaz de circuito de marcación PPP.
- El enlace secundario debe ser un circuito de marcación PPP o una interfaz PPP multienlace.
- Debe habilitar la característica WRS mediante el mandato **enable wrs**.
- Debe habilitar el par primario/secundario mediante el mandato **enable secondary-circuit**.

Nota: Cuando se configura BRS en un enlace primario, que forma parte de un par primario-secundario para la Restauración de WAN, debe configurar BRS en el enlace secundario. Habitualmente, cuando se utiliza la Restauración de WAN, el enlace secundario adopta la identidad del enlace primario. No obs-

tante, esto no es cierto para BRS; por lo tanto, BRS tiene que configurarse tanto en el enlace primario como en el secundario.

Redireccionamiento de WAN

Redireccionamiento de WAN es una función más avanzada. Al utilizar el Redireccionamiento de WAN, configura un enlace primario y otro alternativo. En caso de que el enlace primario falle, se inicia el enlace alternativo. Los protocolos de direccionamiento (por ejemplo, RIP o OSPF) detectan el enlace recién disponible y ajustan las rutas que se utilizarán para reenviar los paquetes.

Para el Redireccionamiento de WAN:

- Existe un emparejamiento entre un enlace primario y otro alternativo.
- Puede configurar varios enlaces primarios para utilizar el mismo enlace alternativo.
- Debe configurar definiciones de protocolo en el enlace alternativo.
- El enlace primario puede ser cualquier enlace en el que puede configurar protocolos direccionables (por ejemplo: IP, IPX). Por ejemplo, el enlace primario puede ser una interfaz LAN, una interfaz serie PPP, Frame Relay o X.25, o un circuito de marcación PPP o Frame Relay. A continuación se incluyen ejemplos de tipos de interfaz que no pueden ser enlaces primarios: interfaces serie SDLC, interfaces serie SRLY y redes de base como V.25bis y RDSI.
- El enlace primario puede ser cualquier enlace en el que puede configurar protocolos direccionables (por ejemplo: IP, IPX) y no es necesario que el tipo de enlace de datos del enlace alternativo coincida con el tipo de enlace de datos del enlace primario. Por ejemplo, el enlace alternativo puede ser una interfaz LAN, una interfaz serie PPP, Frame Relay o X.25, o un circuito de marcación PPP o Frame Relay. A continuación se incluyen ejemplos de tipos de interfaz que no pueden ser enlaces alternativos: interfaces serie SDLC, interfaces serie SRLY y redes de base como V.25bis y RDSI.
- Si el enlace primario es un circuito de marcación, no puede ser un circuito de marcación bajo demanda. Para configurar el circuito de marcación, de tal manera que no sea un circuito de marcación bajo demanda, debe configurarlo con **set idle 0** en ese indicador `Circuit Config` de marcación. Consulte "Configuring and Monitoring Dial Circuits" del manual *Nways Multiprotocol Access Services Guía del usuario de software* para obtener más información.

Los circuitos de marcación I.430, I.431 y Channelized T1/E1 son fijos de manera implícita y, por lo tanto, pueden utilizarse como un primario WRS.

Nota: Los circuitos de marcación I.430/I.431 y Channelized T1/E1 pueden utilizarse como primario WRS sin ninguna configuración explícita.

- El mandato alternativo no puede ser un circuito de marcación bajo demanda (debe configurar **set idle 0** en el circuito de marcación).
- Debe habilitar la característica WRS mediante el mandato **enable wrs**.
- Debe habilitar el par primario/alternativo mediante el mandato **enable alternate-circuit**.
- Opcionalmente, puede configurar períodos de tiempo de estabilización, estabilización de direccionamiento y horas inicial y final de retorno, para controlar la conmutación de vuelta al enlace primario.

- Si el enlace alternativo es X.25, debe utilizar el mandato **national-personality set disconnect-procedure active** al configurar la interfaz X.25 del direccionador que tiene habilitado el Redireccionamiento de WAN, y el mandato **national-personality set disconnect-procedure passive** al configurar la interfaz X.25 del otro direccionador.

Marcación en desbordamiento

La Marcación en desbordamiento es similar al Redireccionamiento de WAN, pero no requiere el fallo del primario para iniciar el enlace alternativo. En cambio, se supervisa la utilización del enlace primario y, si se sobrepasa un umbral, se inicia el enlace alternativo. Además, no todos los protocolos se activan en el enlace alternativo. Sólo se activa IP en el enlace alternativo y otros protocolos siguen utilizando el enlace primario, a menos que el enlace primario se desactive.

Si el enlace primario se desactiva, el Redireccionamiento de WAN toma el relevo y los protocolos configurados en la interfaz alternativa pueden empezar a detectar y utilizar rutas en la interfaz alternativa.

Para la Marcación en desbordamiento:

- La Marcación en desbordamiento utiliza el emparejamiento primario/alternativo de un par de Redireccionamiento de WAN.
- Debe configurar un par de redireccionamiento de WAN para utilizar la Marcación en desbordamiento, y se aplican todas las restricciones existentes de la configuración del Redireccionamiento de WAN.
- El enlace primario de un par de Redireccionamiento de WAN que se utilizará para la Marcación en desbordamiento debe ser Frame Relay.
- Debe utilizar el protocolo de direccionamiento OSPF para utilizar la Marcación en desbordamiento.
- Debe utilizar el mandato **enable dial-on-overflow** para configurar add-threshold y drop-threshold, el intervalo de supervisión de ancho de banda y el tiempo de activación alternativo mínimo.
- Los períodos de tiempo de estabilización, estabilización de direccionamiento, hora inicial de retorno y hora final de retorno no afectan al funcionamiento de la marcación en desbordamiento.

Para obtener más información acerca del Redireccionamiento de WAN, consulte “La característica Redireccionamiento de WAN” en la página 99.

Antes de empezar

Antes de configurar la Restauración de WAN, debe tener los siguientes elementos:

1. Una interfaz serie primaria (línea alquilada) configurada para PPP. Puede utilizar cualquier interfaz serie en el direccionador.
2. Una interfaz con los circuitos de marcación asociados que están configurados en el direccionador. Como red base, puede utilizar una interfaz RDSI o V.25bis.
3. Un circuito de marcación secundario, configurado para la marcación cuando la interfaz primaria se desconecte. Para configurar un circuito de marcación para esto, defina el temporizador de desocupado con el valor cero mediante el

mandato **set idle** en este indicador de marcación `Circuit Config>`. Este mandato evita que el circuito de marcación sea de marcación bajo demanda.

4. Un circuito de marcación secundario en un extremo del enlace configurado sólo para enviar llamadas. Utilice el mandato **set calls outbound** en el indicador `Circuit Config>`.

Nota: No configure ninguna dirección de protocolo en la interfaz secundaria. Las asignaciones de protocolo para la interfaz primaria se utilizan en el enlace secundario (circuito de marcación) cuando está activo.

5. Un circuito de marcación secundario en el otro extremo del enlace configurado sólo para recibir llamadas. Utilice el mandato **set calls inbound** en el indicador `Circuit Config>`.

Procedimiento de configuración para la Restauración de WAN

Esta sección describe los pasos necesarios para configurar la Restauración de WAN. Antes de empezar, utilice el mandato **list device** en el indicador `Config>` para listar los números de interfaz de dispositivos distintos.

Siga estos pasos para configurar la Restauración de WAN en el direccionador:

1. Visualice el indicador `WRS Config>` entrando el mandato **feature wrs** en el indicador `Config>`. Por ejemplo:

```
Config>feature wrs
WAN Restora1 user configuration
WRS Config>
```

2. Asigne un circuito de marcación secundario a la interfaz primaria. Este circuito de marcación actuará como reserva de la interfaz primaria. Por ejemplo:

```
WRS Config>add secondary-circuit
Secondary interface number [0]? 3
Primary interface number [0]? 1
```

3. Habilite la Restauración de WAN en el circuito de marcación secundario que ha añadido. Por ejemplo:

```
WRS Config>enable secondary-circuit
Secondary interface number [0]? 3
```

4. Habilite globalmente la Restauración de WAN en el direccionador. Por ejemplo:

```
WRS Config>enable wrs
```

5. Reinicie el direccionador para que los cambios de configuración entren en vigor.

Configuración de circuito de marcación secundario

Para configurar un circuito de marcación:

1. Determine el número de interfaz de circuito de marcación: para ello, escriba:

```
Config> list device
```

Si no aparece en la lista ninguna interfaz de circuito de marcación PPP, añada una interfaz de circuito de marcación escribiendo lo siguiente:

```
Config> add device dial-circuit
```

```
Adding device as interface 3
Defaulting Data-link protocol to PPP
Use "net 3" command to configure circuit parameters
```

2. Configure la interfaz secundaria (circuito de marcación) para tener el mismo tipo de enlace de datos que la interfaz primaria (PPP) desde el indicador Config>, de la manera siguiente:

```
Config> set data PPP  
Interface Number [0]? 3
```

3. Acceda al indicador de configuración de circuito de marcación (Circuit Config>) entrando **network** *núm-interfaz*.

```
Config> network 3
```

4. Seleccione la interfaz de red base para el circuito de marcación. La red base puede ser V.25bis, o RDSI.

```
Circuit Config> set net 2
```

5. Defina el temporizador de desocupado de circuito de marcación con el valor 0 (0=fijo), de la manera siguiente:

```
Circuit Config> set idle 0
```

6. Defina un extremo de la conexión de reserva para recibir llamadas (por ejemplo, el direccionador A), de la manera siguiente:

```
Circuit Config> set calls inbound
```

7. Defina el otro extremo de la conexión de reserva para iniciar llamadas (por ejemplo, el direccionador B), de la manera siguiente:

```
Circuit Config> set calls outbound
```

Notas:

1. No utilice el mandato **set calls both**. Estas definiciones individuales ayudarán a evitar colisiones de intentos de conexión entrantes y salientes.
2. No configure ninguna dirección de reenvío (por ejemplo, IP, IPX, etc.) en el circuito de marcación. Las asignaciones de protocolo para la interfaz primaria se utilizan en la interfaz secundaria (circuito de marcación) cuando está activa.
3. Para ver las instrucciones de configuración de RDSI, consulte "Using the ISDN Interface" en el manual *Nways Multiprotocol Access Services Guía del usuario de software*.
4. Para ver las instrucciones de configuración de V.25bis, consulte "Using the V.25bis Interface" en el manual *Nways Multiprotocol Access Services Guía del usuario de software*.

Configuración y supervisión de Restauración de WAN

Este capítulo describe los mandatos operativos y de configuración de la Restauración de WAN. Incluye las secciones siguientes:

- “Acceso al proceso de supervisión de la interfaz de Restauración de WAN” en la página 86
- “Mandatos de supervisión de la Restauración de WAN” en la página 86

Nota: Consulte “Configuring and Monitoring Dial Circuits” en el manual *Nways Multiprotocol Access Services Guía del usuario de software* para obtener información acerca de la configuración de circuitos de marcación. Un circuito de marcación puede utilizarse como interfaz al configurar el Redireccionamiento de WAN.

Mandatos de configuración de Restauración de WAN, Redireccionamiento de WAN y Marcación en desbordamiento

Los mandatos de configuración de la Restauración de WAN le permiten crear o modificar la configuración de interfaz de la Restauración de WAN. En esta sección se resumen y se explican los mandatos de configuración de la Restauración de WAN.

La Tabla 9 lista los mandatos de configuración de la Restauración de WAN y sus funciones. Entre estos mandatos en el indicador WRS Config>. Para acceder a WRS Config>, entre **feature wrs** en el indicador Config>.

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxiv.
Add	Añade una correlación de primaria a secundaria (para Restauración de WAN) o de primaria a alternativa (para Redireccionamiento de WAN).
Disable	Inhabilita WRS, una correlación individual de circuito secundario o una correlación de circuito alternativo.
Enable	Habilita WRS, una correlación individual de circuito secundario o una correlación de circuito alternativo.
List	Visualiza la configuración actual de Restauración.
Remove	Elimina una correlación de primaria a secundaria o una correlación de primaria a alternativa creada por add.
Set	Define los valores para los temporizadores de estabilización, estabilización de direccionamiento y hora de retorno.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiv.

Add

Utilice el mandato **add** para identificar un circuito de marcación secundario o alternativo, o una interfaz de enlace alquilado para un enlace serie primario.

Sintaxis:

```
add                alternate-circuit  
                    secondary-circuit
```

alternate-circuit

El mandato **add alternate-circuit** vincula una interfaz alternativa con una interfaz primaria para propósitos de Redireccionamiento de WAN. Puede asignar varias interfaces primarias a una única interfaz alternativa. No es necesario que el tipo de enlace alternativo sea el mismo que el tipo de enlace primario (por ejemplo, el tipo de enlace alternativo puede ser un circuito de marcación PPP, mientras que el tipo de enlace primario puede ser una línea alquilada Frame Relay).

Ejemplo:

```
WRS Config>add alt  
Alternate interface number [0]? 6  
Primary interface number [0]? 1
```

Alternate interface number

Es el número de interfaz asignado anteriormente a la interfaz alternativa. Cualquier interfaz LAN, interfaz serie PPP, Frame Relay o X.25, o un circuito de marcación Frame Relay, puede ser una interfaz alternativa elegible. El valor por omisión es 0.

Primary interface number

Es el número de interfaz de la interfaz primaria asignada anteriormente, cuando se añadió el dispositivo. Una interfaz primaria puede ser cualquier interfaz LAN definida anteriormente, una interfaz serie PPP, Frame Relay o X.25, o un circuito de marcación PPP o Frame Relay. El valor por omisión es 0.

secondary-circuit

El mandato **add secondary-circuit** vincula una interfaz secundaria a una interfaz primaria para los fines de la Restauración de WAN. Es preciso haber configurado anteriormente ambas interfaces. Sólo puede asignar una interfaz secundaria a una primaria y viceversa.

Ejemplo:

```
WRS Config>add secondary-circuit  
Secondary interface number [0]? 4  
Primary interface number [0]? 1
```

Secondary interface number

Es el número de interfaz de circuito de marcación asignado anteriormente a la interfaz secundaria cuando se añadió el dispositivo. Cualquier circuito de marcación PPP o interfaz PPP multienlace puede ser una interfaz secundaria. El valor por omisión es 0.

Primary interface number

Es el número de interfaz de la interfaz primaria asignada anteriormente, cuando se añadió el dispositivo. Una interfaz

primaria puede ser cualquier línea alquilada definida anteriormente ejecutando PPP. El valor por omisión es 0.

Disable

Utilice el mandato **disable** para inhabilitar la función de Restauración de WAN, o para inhabilitar un par primario/secundario para la Restauración de WAN, o para inhabilitar un par primario/alternativo para el Redireccionamiento de WAN, o para inhabilitar la Marcación en desbordamiento para un par primario/alternativo.

Sintaxis:

```
disable          alternate-circuit
                  dial-on-overflow
                  secondary-circuit
                  wRS
```

alternate-circuit *núm-interfaz*

Inhabilita el par primario/alternativo para el Redireccionamiento de WAN.

Ejemplo:

```
WRS Config> disable alternate-circuit
Alternate interface number [0]? 6
```

Alternate interface number

Es el número de la interfaz alternativa configurada anteriormente con el mandato **add alternate-circuit**. El valor por omisión es 0.

dial-on-overflow *núm-interfaz-alt*

Inhabilita la marcación en desbordamiento para todos los pares primario/alternativo utilizando una alternativa especificada.

Ejemplo:

```
WRS Config> disable dial-on-overflow
alternate interface number [0]? 6
```

Alternate interface number

Es el número de la interfaz alternativa configurada anteriormente con el mandato **add alternate-circuit**. El valor por omisión es 0.

secondary-circuit *núm-interfaz*

Inhabilita la restauración de una interfaz primaria determinada por su interfaz secundaria asociada, hasta el siguiente mandato **enable secondary-circuit** en la consola WRS. Es preciso haber configurado anteriormente ambas interfaces y tenerlas vinculadas en la configuración de WRS.

Ejemplo:

```
WRS Config> disable secondary-circuit
Secondary interface number [0]? 3
```

Secondary interface number

Es el número de la interfaz secundaria configurada anteriormente con el mandato **add secondary-circuit**. El valor por omisión es 0.

Configuración de Restauración de WAN

wrs Inhabilita globalmente la característica Restauración de WAN en el direccionador. Esto quiere decir que el Redireccionamiento de WAN y Marcación en desbordamiento también se inhabilitan.

Enable

Utilice el mandato **enable** para habilitar la función de Restauración de WAN, o para habilitar un par primario/secundario para la Restauración de WAN, o para habilitar un par primario/alternativo para el Redireccionamiento de WAN, o para habilitar la marcación en desbordamiento para un par primario/alternativo.

Sintaxis:

enable alternate-circuit
 dial-on-overflow
 secondary-circuit

 wrs

alternate-circuit *núm-interfaz*

Habilita un circuito alternativo

Ejemplo:

```
WRS Config>enable alternate-circuit
Alternate interface number [0]? 6
```

Alternate interface number

Es el número de la interfaz alternativa configurada anteriormente con el mandato **add alternate-circuit**. El valor por omisión es 0.

dial-on-overflow

Habilita la marcación en desbordamiento y le permite definir parámetros que controlan el funcionamiento de la marcación en desbordamiento.

Ejemplo:

```
WRS>enable dial-on-overflow

For dial-on-overflow, only IP traffic can overflow to the alternate
interface.
Primary interface number ]0]? 1
add-threshold (1-100% utilization) [90]?
drop-threshold(0-99% utilization) [60]?
bandwidth test interval(10-200 seconds) [15]?
minimum time to keep the alternate up (20-21600 sec.) [300]?
Dial-on overflow is enabled.
Remember to configure the primary interface's line speed!
```

Primary interface number

Es el número de interfaz de la interfaz primaria para la que ha habilitado la marcación en desbordamiento. El valor por omisión es 0.

add-threshold

Determina cuándo se activará una interfaz alternativa para el ancho de banda adicional. Este valor debe expresarse como porcentaje de la velocidad de línea configurada de la interfaz primaria. El valor por omisión es 90%.

drop-threshold

Determina cuándo una interfaz alternativa ya no es necesaria para el ancho de banda adicional. Este valor debe expresarse

sarse como porcentaje de la velocidad de línea configurada de la interfaz primaria. El valor por omisión es 60%.

bandwidth monitoring interval

Determina con cuánta frecuencia se supervisa el ancho de banda de la interfaz primaria para *add-threshold* y *drop-threshold*. El valor por omisión es 15 segundos.

Minimum time to keep alternate up

Este período de tiempo tiene que incluir tiempo suficiente para que los direccionadores establezcan la nueva ruta cuando el tráfico IP en el direccionador local se redirija a la interfaz alternativa. El valor por omisión es 5 minutos.

secondary-circuit *núm-interfaz*

Habilita la restauración de un enlace primario por el enlace secundario indicado.

Ejemplo:

```
WRS Config>enable secondary-circuit  
Secondary interface number [0]? 3
```

Secondary interface number

Es el número de la interfaz secundaria configurada anteriormente con el mandato **add secondary-circuit**. El valor por omisión es 0.

wrs Habilita globalmente la característica Restauración de WAN en el direccionador. Esto quiere decir que, si se configuran el Redireccionamiento de WAN y la Marcación en desbordamiento, también se habilitan.

List

Utilice el mandato **list** para visualizar información de configuración global para la característica y visualizar información de configuración para los pares primario-secundario de la Restauración de WAN, los pares primario-alternativo del Redireccionamiento de WAN y la Marcación en desbordamiento.

Sintaxis:

list

Ejemplo:

Configuración de Restauración de WAN

```
WRS Config>list all
WAN Restoral is enabled.
Default Stabilization Time:      0 seconds
Default First Stabilization Time: 0 seconds
```

Primary Interface	Secondary Interface	Secondary Enabled	Alt. Enabled	1st Stab	Subseq Stab	TOD Start	Revert Stop	Back Stop	Stab
4 - WAN PPP	7 - PPP Dial Circuit	No							
1 - WAN Frame Re	2 - WAN Frame Relay	Yes	dflt	dflt	Not Set	Not Set	Not Set	Not Set	15

```
Dial-on-overflow is enabled.
Primary add- drop- test minimum
Interface threshold threshold interval alt up time
-----
1          29%    20%    15 sec.  300 sec.
```

Remove

Utilice el mandato **remove** para suprimir la correlación de una interfaz alternativa o secundaria (de seguridad) con la interfaz primaria.

Sintaxis:

```
remove          alternate-circuit
                  secondary-circuit
```

alternate-circuit *alternate-interface# primary-interface#*

Elimina la correlación de una interfaz alternativa (de seguridad) con una interfaz primaria para el Redireccionamiento de WAN. Es preciso haber asignado y vinculado anteriormente ambas interfaces mediante el mandato **add alternate-circuit**.

Alternate-interface#

Es el número de la interfaz alternativa configurada anteriormente con el mandato **add alternate-circuit**. El valor por omisión es 0.

Primary-interface#

Es el número de interfaz de la interfaz primaria vinculada anteriormente con la alternativa que se elimina. El valor por omisión es 0.

Ejemplo:

```
WRS Config> remove alternate-circuit
Alternate interface number [0]? 3
Primary interface number [0]? 1
```

secondary-circuit *secondary-interface# primary-interface#*

Elimina la correlación de una interfaz secundaria (de seguridad) con una interfaz primaria para la Restauración de WAN. Es preciso haber asignado y vinculado anteriormente ambas interfaces mediante el mandato **add secondary-circuit**.

Secondary-interface#

Es el número de la interfaz secundaria configurada anteriormente con el mandato **add secondary-circuit**. El valor por omisión es 0.

Primary-interface#

Es el número de interfaz de la interfaz primaria vinculada anteriormente con la secundaria que se elimina. El valor por omisión es 0.

Ejemplo:

```
WRS Config> remove secondary-circuit
Secondary interface number [0]? 3
Primary interface number [0]? 1
```

Set

Utilice el mandato **set** para definir los parámetros para el Redireccionamiento de WAN.

Sintaxis:

```
set ?          default
               first-stabilization
               routing-stabilization
               stabilization
               start-time-of-day-revert-back
               stop-time-of-day-revert-back
```

default Utilice el mandato **set default** para definir los valores por omisión que van a ser utilizados por los enlaces que no hayan configurado los períodos de tiempo de estabilización y primera estabilización.

first-stabilization

Define el valor de primera estabilización por omisión que va a utilizarse para los enlaces para los que no se ha configurado un período de tiempo de primera estabilización.

```
WRS Config>set default first
Default first primary stabilization time (0 - 3600 seconds) [0]? 20
```

stabilization

Define el valor de estabilización por omisión que va a utilizarse para los enlaces para los que no se ha configurado un período de tiempo de estabilización.

```
WRS Config>set default stab
Default primary stabilization time (0 - 3600 seconds) [0]? 30
```

first-stabilization

Define el número de segundos en la inicialización del direccionador, antes de que el direccionamiento para este enlace primario se conmute al enlace alternativo, si el enlace primario no está activado.

Ejemplo:

```
WRS Config>set first
Primary interface number [0]? 1
First primary stabilization time (0 - 3600 seconds -1 = default) [-1]?
```

Primary interface number

Es el número de interfaz primaria de la interfaz primaria para la que se define la primera estabilización. El valor por omisión es 0.

First primary stabilization time

Período de tiempo de estabilización para esta interfaz primaria. El valor por omisión es 1.

routing-stabilization

Define el valor de estabilización de direccionamiento. Este parámetro define el número de segundos que tanto el enlace primario como el alternativo permanecen activados, después de que se haya encontrado que el enlace primario está activado y que el temporizador de estabilización, en caso de existir, ya ha caducado. Se proporciona el período de tiempo de estabilización de direccionamiento para que los protocolos de direccionamiento, como OSPF o RIP, tengan tiempo suficiente para reconocer la disponibilidad de la nueva ruta. Sin el temporizador de estabilización de direccionamiento, el tráfico puede interrumpirse durante unos segundos mientras se ha inhabilitado la ruta alternativa pero todavía no se ha descubierto la ruta primaria.

Si el enlace alternativo estaba activado antes que el redireccionamiento, permanece activado y se pasa por alto el temporizador de estabilización de direccionamiento. Si el enlace alternativo se desactivó antes que el redireccionamiento o durante el mismo, permanece desactivado y se pasan por alto el temporizador de estabilización de direccionamiento y el temporizador de estabilización.

```
WRS Config>set routing-stabilization
Primary interface number [0]? 1
Routing stabilization timer (0 - 3600 seconds) [0]?
```

Primary interface number

Valores válidos: de 0 al número de interfaces configuradas en el direccionador

Valor por omisión: 0

Routing-stabilization timer

Valores válidos: 1 a 3600 segundos

Valor por omisión: 0

stabilization

Define el número de segundos necesario después de que se detecte por primera vez que el enlace primario está activado, antes de que empiece el proceso de reinicializar el direccionamiento en el enlace primario. Cuando caduque el temporizador de estabilización, se desactivará el enlace alternativo, a menos que se haya configurado el temporizador de estabilización de direccionamiento. El temporizador de estabilización de direccionamiento empezará tan pronto como caduque el temporizador de estabilización y conservará activados los enlaces primario y alternativo el tiempo suficiente para mantener el tráfico en el enlace alternativo, mientras los protocolos de direccionamiento, como OSPF y RIP, restablecen la ruta a través del enlace primario.

Ejemplo:

```
WRS Config>set first
Primary interface number [0]? 1
Primary stabilization time (0 - 3600 seconds -1 = default) [-1]?
```


Primary interface number

Es el número de interfaz primaria de la interfaz primaria para la que se define la estabilización. El valor por omisión es 0.

Primary stabilization time

Período de tiempo de estabilización para la interfaz primaria. El valor por omisión es 1.

start-time-of-day-revert-back

Hora más temprana del día en que el direccionador puede conmutar de vuelta a la ruta primaria. El direccionador puede retornar a la primaria en cualquier momento entre las horas indicadas por start-time-of-day-revert-back y stop-time-of-day-revert-back. El retorno a la ruta primaria sólo se producirá si está activada y se cumplen los parámetros de estabilización. El valor por omisión es 0.

Ejemplo:

```
WRS Config>set start Primary interface number [0]? 1
Time-of-Day revert back window start (1 - 24 hours, 0 = not configured) [0] 3
Start time-of-day revert back configured. Remember to configure stop time-of-day
```

Primary interface number

Es el número de interfaz primaria de la interfaz primaria para la que ha definido la primera estabilización. El valor por omisión es 0.

Time-of-day-revert-back-window start

Esta hora marca la hora inicial de la ventana de retorno. El direccionador puede retornar a la interfaz primaria en cualquier momento entre las horas indicadas por start-time-of-day-revert-back y stop-time-of-day-revert-back. El retorno a la interfaz primaria sólo se producirá si está activada y se cumplen los parámetros de estabilización. El valor por omisión es 1.

stop-time-of-day-revert-back

Esta hora marca la hora final de la ventana de retorno. El direccionador puede retornar a la interfaz primaria en cualquier momento entre las horas indicadas por start-time-of-day-revert-back y stop-time-of-day-revert-back. El retorno a la interfaz primaria sólo se producirá si está activada y se cumplen los parámetros de estabilización. El valor por omisión es 1.

Ejemplo:

```
WRS Config>set stop
Primary interface number [0]? 1
Time-of-Day revert back window stop (1 - 24 hours, 0 = not configured) [0]?5
```

Primary interface number

Es el número de interfaz primaria de la interfaz primaria para la que ha definido la primera estabilización. El valor por omisión es 0.

Time-of-day-revert-back-window stop

Esta hora marca la hora final de la ventana de retorno. El direccionador puede retornar a la interfaz primaria en cualquier momento entre las horas indicadas por start-time-of-day-revert-back y stop-time-of-day-revert-back. El retorno a la interfaz primaria sólo se producirá si está activada y se

cumplen los parámetros de estabilización. El valor por omisión es 1.

Acceso al proceso de supervisión de la interfaz de Restauración de WAN

Para acceder al proceso de supervisión de la interfaz de Restauración de WAN, entre el siguiente mandato en el indicador GWCON (+):

+ feature wrs

Mandatos de supervisión de la Restauración de WAN

Los mandatos de supervisión de la Restauración de WAN (WRS) le permiten supervisar el estado de los pares primario-secundario de la Restauración de WAN, los pares primario-alternativo del Redireccionamiento de WAN y la Marcación en desbordamiento. Las modificaciones que se efectúen en el estado operativo de Restauración de WAN, Redireccionamiento de WAN y Marcación en desbordamiento, hechas a través de la interfaz de supervisión, no se mantendrán entre los reinicios del direccionador.

Acceda al indicador WRS entrando **feature wrs** en el indicador GWCON (+). La Tabla 10 lista los mandatos de WRS y sus funciones, mientras que las secciones siguientes explican los mandatos.

<i>Tabla 10. Mandatos de supervisión de la Restauración de WAN</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 el apartado "Cómo obtener ayuda" en la página xxxiv.
Clear	Borra las estadísticas de supervisión visualizadas mediante el mandato list .
Disable	Inhabilita WRS, un secundario o alternativo individual, o la marcación en desbordamiento.
Enable	Habilita WRS, un secundario o alternativo individual, o la marcación en desbordamiento.
List	Visualiza la información de supervisión en un circuito alternativo o secundario, o en todos ellos.
Set	Define los valores para los temporizadores de estabilización, estabilización de direccionamiento y hora de retorno.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página xxxiv.

Clear

Utilice el mandato **clear** para borrar las estadísticas de Restauración de WAN, Redireccionamiento de WAN y marcación en desbordamiento, que se visualizan mediante el mandato **list**.

Sintaxis:

clear

Nota: Este mandato borra *Longest restoral period*, pero no *Most recent restoral period*. Para la visualización en pantalla, consulte el ejemplo incluido en el mandato **list**.

Disable

Utilice el mandato **disable** para inhabilitar por completo la característica Restauración de WAN, inhabilitar la restauración de una interfaz primaria determinada por su interfaz secundaria asociada, inhabilitar una interfaz alternativa o inhabilitar la marcación en desbordamiento.

Sintaxis:

```
disable          alternate-circuit
                  dial-on-overflow
                  secondary-circuit
                  wrs
```

alternate-circuit

Inhabilita el par primario/alternativo para el Redireccionamiento de WAN. Varios pares pueden utilizar el mismo alternativo. Este mandato inhabilita todos los pares que utilizan el circuito alternativo especificado.

Ejemplo:

```
WRS>disable alternate-circuit
Alternate circuit number [0]? 6
```

Alternate circuit number

Es el número del circuito alternativo. El valor por omisión es 0.

dial-on-overflow

Inhabilita la marcación en desbordamiento para el par primario/alternativo especificado, sin modificar el estado habilitado/inhabilitado del Redireccionamiento de WAN para ese par. Si la marcación en desbordamiento realiza el direccionamiento de forma activa, se termina al caducar el siguiente intervalo de supervisor.

secondary-circuit

Inhabilita la restauración de una interfaz primaria determinada por su interfaz secundaria asociada, hasta el siguiente mandato **restart**, **reload** o **enable secondary-circuit**. Es preciso haber configurado anteriormente ambas interfaces y tenerlas vinculadas en la configuración de WRS.

Normalmente, en **talk 5** (GWCON), el mandato **disable** hace que la interfaz esté inactiva y permanezca así. Sin embargo, para la secundaria de la Restauración de WAN, éste no es el caso. El mandato **disable**, aplicado a la interfaz secundaria, no inhabilita la interfaz. Sólo inhabilita la llamada actual (es decir, hace que se desconecte cualquier llamada activa). Para inhabilitar la utilización del circuito secundario, tendrá que ejecutar **disable secondary-circuit** en el indicador de supervisión de la Restauración de WAN e inhabilitar la interfaz secundaria en el indicador GWCON de nivel superior. **Ejemplo:**

```
WRS>disable secondary-circuit
Secondary interface number [0]? 3
```

Configuración de Restauración de WAN

Secondary interface number

Es el número de la interfaz secundaria configurada anteriormente con el mandato **add secondary-circuit**. El valor por omisión es 0.

wrs Al inhabilitar WRS se inhabilitan la Restauración de WAN, el Redireccionamiento de WAN y la Marcación en desbordamiento en el direccionador, hasta el siguiente mandato **restart**, **reload** o **enable WRS**.

Enable

Utilice el mandato **enable** para habilitar la interfaz de Restauración de WAN, la restauración de un enlace primario por un circuito secundario, un circuito alternativo o la marcación en desbordamiento.

Sintaxis:

```
enable          alternate-circuit  
                  dial-on-overflow  
                  secondary-circuit  
                  wrs
```

alternate-circuit

Habilita los pares primario/alternativo para el Redireccionamiento de WAN para todos los pares utilizando el alternativo especificado.

Ejemplo:

```
WRS> enable alternate-circuit  
Alternate circuit number [0]? 3
```

Alternate circuit number

Es el número de interfaz del circuito alternativo. El valor por omisión es 0.

dial-on-overflow

Habilita la marcación en desbordamiento y le permite definir parámetros que controlan la marcación en desbordamiento. Opcionalmente, le permite que el protocolo IP se conmute inmediatamente al alternativo, como si se hubiera cruzado el valor de umbral de adición.

Ejemplo:

```
WRS> dial-on-overflow  
  
For dial-on-overflow, only IP traffic can overflow to the alternate interface.  
Primary interface number [0]? 1  
add-threshold (1-100% utilization) [90]?  
drop-threshold(0-99% utilization) [60]?  
bandwidth test interval(10-200 seconds) [15]?  
minimum time to keep the alternate up (20-21600 sec.) [300]?  
Dial-on overflow is enabled.  
Remember to configure the primary interface's line speed!  
  
Do you want to switch IP traffic to the alternate now?(Yes or [No]):  
WRS>
```

secondary-circuit

Habilita la restauración de un enlace primario por el enlace secundario indicado.

Ejemplo:

```
WRS> enable secondary-circuit  
Secondary interface number [0]? 3
```

Secondary interface number

Es el número de la interfaz secundaria configurada anteriormente con el mandato **add secondary-circuit**. El valor por omisión es 0.

wrs Habilita la característica Restauración de WAN en el direccionador. Esta característica tiene que habilitarse para realizar la Restauración de WAN, el Redireccionamiento de WAN o la Marcación en desbordamiento.

Set

Utilice el mandato **set** para definir los parámetros para el Redireccionamiento de WAN.

Sintaxis:

```
set ?          default
               first-stabilization
               routing-stabilization
               stabilization
               start-time-of-day-revert-back
               stop-time-of-day-revert-back
```

default Utilice el mandato **set default** para definir los valores por omisión que van a ser utilizados por los enlaces que no hayan configurado los períodos de tiempo de estabilización y primera estabilización.

Ejemplo:

```
WRS Config>set default ?
FIRST-STABILIZATION
STABILIZATION
```

first-stabilization

Define el valor de primera estabilización por omisión que va a utilizarse para los enlaces para los que no se ha configurado un período de tiempo de primera estabilización.

```
WRS Config>set default first
Default first primary stabilization time (0 - 3600 seconds) [0]? 20
```

stabilization

Define el valor de estabilización por omisión que va a utilizarse para los enlaces para los que no se ha configurado un período de tiempo de estabilización.

```
WRS Config>set default stab Default primary stabilization time (0 - 3600 seconds) [0]? 30
```

first-stabilization

Define el número de segundos en la inicialización del direccionador, antes de que el direccionamiento para este enlace primario se conmute al enlace alternativo, si el enlace primario no está activado.

Ejemplo:

```
WRS Config>set first
Primary interface number [0]? 1
First primary stabilization time (0 - 3600 seconds -1 = default) [-1]?
```

Primary interface number

Es el número de interfaz primaria de la interfaz primaria para la que ha definido la primera estabilización. El valor por omisión es 0.

First primary stabilization time

Período de tiempo de estabilización para esta interfaz primaria. El valor por omisión es 1.

routing-stabilization

Define el valor de estabilización de direccionamiento. Este parámetro define el número de segundos que tanto el enlace primario como el alternativo permanecen activados, después de que se haya encontrado que el enlace primario está activado y que el temporizador de estabilización, en caso de existir, ya ha caducado. Se proporciona el período de tiempo de estabilización de direccionamiento para que los protocolos de direccionamiento, como OSPF o RIP, tengan tiempo suficiente para reconocer la disponibilidad de la nueva ruta. Sin el temporizador de estabilización de direccionamiento, el tráfico puede interrumpirse durante unos segundos mientras se ha inhabilitado la ruta alternativa pero todavía no se ha descubierto la ruta primaria.

Si el enlace alternativo estaba activado antes que el redireccionamiento, permanece activado y se pasa por alto el temporizador de estabilización de direccionamiento. Si el enlace alternativo se desactivó antes que el redireccionamiento o durante el mismo, permanece desactivado y se pasan por alto el temporizador de estabilización de direccionamiento y el temporizador de estabilización.

```
WRS Config>set routing-stabilization
Primary interface number [0]? 1
Routing stabilization timer (0 - 3600 seconds) [15]?
```

Primary interface number

Valores válidos: de 0 al número de interfaces configurados en el direccionador

Valor por omisión: 0

Routing-stabilization timer

Valores válidos: 1 a 3600 segundos

Valor por omisión: 0

stabilization

Define el número de segundos necesario después de que se detecte por primera vez que el enlace primario está activado, antes de que empiece el proceso de reinicializar el direccionamiento en el enlace primario. Cuando caduque el temporizador de estabilización, se desactivará el enlace alternativo, a menos que se haya configurado el temporizador de estabilización de direccionamiento. El temporizador de estabilización de direccionamiento empezará tan pronto como caduque el temporizador de estabilización y conservará activados los enlaces primario y alternativo el tiempo suficiente para mantener el tráfico en el enlace alternativo, mientras los protocolos de direccionamiento, como OSPF y RIP, restablecen la ruta a través del enlace primario.

Ejemplo:

```
WRS Config>set first Primary interface number [0]? 1
Primary stabilization time (0 - 3600 seconds -1 = default) [-1]?
```

Primary interface number

Es el número de interfaz primaria de la interfaz primaria para la que se define la estabilización. El valor por omisión es 0.

Primary stabilization time

Período de tiempo de estabilización para la interfaz primaria. El valor por omisión es 1.

start-time-of-day-revert-back

Define la hora más temprana del día en que el direccionador puede conmutar de vuelta a la ruta primaria. El direccionador puede retornar a la primaria en cualquier momento entre las horas indicadas por start-time-of-day-revert-back y stop-time-of-day-revert-back. El retorno a la ruta primaria sólo se producirá si está activada y se cumplen los parámetros de estabilización. El valor por omisión es 0.

Ejemplo:

```
WRS Config>set start
Primary interface number [0]? 1
Time-of-Day revert back window start (1 - 24 hours, 0 = not configured) [0] 3
Start time-of-day revert back configured. Remember to configure stop time-of-day
```

Primary interface number

Es el número de interfaz primaria de la interfaz primaria para la que ha definido la primera estabilización. El valor por omisión es 0.

Time-of-day-revert-back-window start

Esta hora marca la hora inicial de la ventana de retorno. El direccionador puede retornar a la interfaz primaria en cualquier momento entre las horas indicadas por start-time-of-day-revert-back y stop-time-of-day-revert-back. El retorno a la interfaz primaria sólo se producirá si está activada y se cumplen los parámetros de estabilización. El valor por omisión es 1.

stop-time-of-day-revert-back

Esta hora marca la hora final de la ventana de retorno. El direccionador puede retornar a la interfaz primaria en cualquier momento entre las horas indicadas por start-time-of-day-revert-back y stop-time-of-day-revert-back. El retorno a la interfaz primaria sólo se producirá si está activada y se cumplen los parámetros de estabilización. El valor por omisión es 1.

Ejemplo:

```
WRS Config>set stop Primary interface number [0]? 1
Time-of-Day revert back window start (1 - 24 hours, 0 = not configured) [0] 5
```

Primary interface number

Es el número de interfaz primaria de la interfaz primaria para la que ha definido la primera estabilización. El valor por omisión es 0.

Time-of-day-revert-back-window stop

Esta hora marca la hora final de la ventana de retorno. El direccionador puede retornar a la interfaz primaria en cual-

Configuración de Restauración de WAN

quier momento entre las horas indicadas por `start-time-of-day-revert-back` y `stop-time-of-day-revert-back`. El retorno a la interfaz primaria sólo se producirá si está activada y se cumplen los parámetros de estabilización. El valor por omisión es 1.

List

Utilice el mandato **list** para visualizar la información de supervisión en uno de los pares primario-secundario de la Restauración de WAN o en todos ellos, o en uno de los pares primario-alternativo del Redireccionamiento de WAN o en todos ellos.

Sintaxis:

```
list          all
                alternate-circuit
                secondary-circuit
                summary
```

all Proporciona información de resumen, seguida por la información específica para cada interfaz secundaria.

Ejemplo:

```
list all
WAN Restoral/Re-route is enabled with 2 circuits configured
Total restoral attempts =          7 completions =          7
Total packets forwarded =          39
Longest completed restoral period in hrs:min:sec    0:03:27

Total overflow attempts =          20 completions =          19
Longest completed overflow period in hrs:min:sec    0:05:00

-----
Primary      Secondary  Restoral  Restoral  Current/Longest
Net Interface Net Interface Enabled   Active   Duration
-----
 4  PPP/0     7  PPP/1     No       No       00:03:27/ 00.06.00

-----
Primary      Alternate  Re-route/ Re-route/  Recent
Net Interface Net Interface Enabled   Active   Reroute/Overflow
-----
 1  FR/0      2  FR/1     Yes/Yes  No /No   00:00:56/ 00:05:00
```

Total restoral attempts

Número de veces que ha fallado el enlace primario, haciendo que el direccionador intente activar un enlace secundario.

Completions

Número de intentos satisfactorios de restauración cuando se activó y se utilizó el enlace secundario.

Total packets forwarded

Número total de paquetes reenviados a través de la interfaz secundaria. Es la suma de ambas direcciones y es acumulativo respecto a todas las restauraciones satisfactorias, hasta que se emita el mandato de reiniciar o borrar las estadísticas de la restauración.

Longest Completed Restoral Period

Este campo visualiza, en horas, minutos y segundos, la mayor cantidad de tiempo que estaba operando la restauración, sin contar su utilización actual.

Total Overflow Attempts

Número de intentos debido a un desbordamiento.

Completions

Número de intentos satisfactorios de desbordamiento cuando se activó y se utilizó el enlace secundario.

Longest Completed Overflow Period

Visualiza, en horas, minutos y segundos, la mayor cantidad de tiempo que estaba operando el desbordamiento, sin contar su utilización actual.

Primary Net Interface

La interfaz para la que la interfaz secundaria asociada actúa como seguridad.

Secondary Net Interface

Circuito de marcación que se utiliza como seguridad para la interfaz primaria asociada.

Restoral Enabled

Indica que la restauración de esta interfaz primaria está habilitada actualmente.

Restoral Active

Indica si la restauración está activa (Yes o No).

Current/Longest Duration

Indica, en horas, minutos y segundos, la duración actual y la más larga que la interfaz de red secundaria estuvo activa.

Primary Net Interface

La interfaz para la que la interfaz alternativa asociada actúa como seguridad.

Alternate Net Interface

La interfaz que se utiliza como alternativa de seguridad para la interfaz primaria asociada.

Re-route/Overflow Enabled

Indica si se habilita el redireccionamiento y el desbordamiento (Yes o No).

Re-route/Overflow Active

Indica si el redireccionamiento y el desbordamiento están activos (Yes o No).

Recent Re-route Overflow Duration

Indica, en horas, minutos y segundos, la duración reciente del redireccionamiento y del desbordamiento de la interfaz de red alternativa.

Alternate-circuit

Proporciona totales para un circuito alternativo. Permite que el operador de supervisión recupere el estado de Redireccionamiento de WAN y las estadísticas asociadas para cada interfaz alternativa y su correlación primaria asociada.

Ejemplo:

```
WRS>1i alt 7
Primary 1:FR/0 Frame Relay V.35/V.36
Alternate 7:PPP/1 Point to Point V.25bis Dial Circuit
reroute Enabled, currently inactive
overflow Enabled, currently inactive
Primary first stabilization time: default (0 seconds)
Primary stabilization time: default (0 seconds)
Routing-stabilization time: 15 seconds
Time-of-day revert back not configured: start = 0, stop = 0
Restored 0 times (0 attempts)
Overflow 0 times (0 attempts)
```

Primary Interface

La interfaz para la que esta interfaz alternativa asociada actúa como seguridad.

Alternate Interface

Circuito de marcación que se utiliza como seguridad para la interfaz primaria asociada.

Reroute Enabled

Indica si el redireccionamiento de esta interfaz primaria está habilitado actualmente o no.

Overflow Enabled

Indica si el desbordamiento de esta interfaz primaria está habilitada actualmente o no.

Primary first stabilization

Número de segundos en la inicialización del direccionador, antes de que el direccionamiento para este enlace primario se conmute al enlace alternativo, si el enlace primario no está activado.

First stabilization

Número de segundos necesario después de que se detecte por primera vez que el enlace primario está activado, antes de que el direccionamiento se conmute de vuelta desde el enlace alternativo al primario. El direccionamiento a través del enlace alternativo continúa hasta que el enlace primario permanezca activado para este número de segundos.

Routing stabilization

Número de segundos necesario después de que el direccionamiento se conmute de vuelta al enlace primario, antes de que se desconecte el enlace alternativo. Durante este período de tiempo, tanto el enlace primario como el alternativo permanecen activados. Este intervalo se proporciona para permitir que los protocolos de direccionamiento, como OSPF y RIP, reconozcan la disponibilidad de la ruta a través de la interfaz primaria.

Time-of-day revert back

Hora del día en que el direccionador puede conmutar de vuelta a la ruta primaria. El direccionador puede retornar a la primaria en cualquier momento entre las horas indicadas por start-time-of-day-revert-back y stop-time-of-day-revert-back. El retorno a la ruta primaria sólo se producirá si está activada y se cumplen los parámetros de estabilización. El valor por omisión es 0.

Restored times

Número de intentos para volver a direccionar la interfaz primaria.

Overflow times

Número de intentos de marcación en desbordamiento.

secondary-circuit

Proporciona totales para cada circuito secundario. Permite que el operador de supervisión recupere el estado de la Restauración de WAN y las estadísticas asociadas para cada interfaz secundaria y su correlación primaria asociada.

Ejemplo:

```
list secondary-circuit
Secondary interface number [0]? 1
```

Primary Interface	Secondary Interface	Secondary Enabled
1 PPP/0 Point to Poi	3 PPP/1 Point to Poi	Yes

```
Router primary interface state = Up
Router secondary interface state = Available
Restoral Statistics:
```

```
Primary restoral attempts =      6  completions =  5
Restoral packets forwarded =   346
Most recent restoral period in hrs:min:sec      00:08:20
```

Primary Interface

Interfaz para la que esta interfaz secundaria asociada actúa como seguridad.

Secondary Interface

Circuito de marcación que se utiliza como seguridad para la interfaz primaria asociada.

Secondary Enabled

Indica si la restauración de esta interfaz primaria está habilitada actualmente o no.

Router Primary Interface State

Indica que el estado de la interfaz primaria es uno de los siguientes:

Up - Indica que el enlace está activado.

Down - Indica que el enlace está desactivado.

Disabled - Indica que el operador ha inhabilitado el enlace.

Not present - Indica que el enlace está configurado, pero hay un problema de hardware.

Router Secondary Interface State

Indica que el estado de la interfaz secundaria asociada es uno de los siguientes:

Up - Indica que el enlace está activado.

Down - Indica que el enlace está desactivado. Esto también se produce cuando la red base para el secundario está inhabilitado en el indicador Config> o en la consola del operador.

Configuración de Restauración de WAN

Available - Indica que el enlace está en la modalidad de espera.

Testing - Indica que el enlace está en proceso de establecer una conexión.

Restoral Statistics:

Primary Restoral Attempts

Número de veces que ha fallado el enlace primario, haciendo que el direccionador intente activar un enlace secundario.

Restoral Packets forwarded

Este campo indica el número total de paquetes reenviados.

Most Recent Restoral Period

Esto indica cuánto tiempo ha estado activado el enlace secundario, la última vez que se utilizó o la duración del uso actual de la restauración.

summary Proporciona totales para cada circuito secundario.

Ejemplo:

```
list summary
WAN Restoral is enabled with 3 circuit(s) configured

Total restoral attempts =      3 completions =      2
Total packets forwarded =    346
Longest restoral period in hrs:min:sec  00:08:20

Primary Interface and State      Secondary Interface and State
-----
1 PPP/0 - Up                    3 PPP/1 - Available
```

Total restoral attempts

Número de veces que ha fallado el enlace primario, haciendo que el direccionador intente activar un enlace secundario.

Completions

Número de intentos satisfactorios de restauración cuando se activó y se utilizó el enlace secundario.

Total packets forwarded

Número total de paquetes reenviados a través de la interfaz secundaria. Es la suma de ambas direcciones y es acumulativo respecto a todos los períodos de restauración, hasta que se utilice el mandato de reiniciar o borrar las estadísticas de la restauración.

Longest restoral period

Este campo visualiza, en horas, minutos y segundos, la mayor cantidad de tiempo que se estaba utilizando la restauración, sin contar su utilización actual.

Primary Interface and State

La interfaz para la que la interfaz secundaria asociada actúa como seguridad. Los estados válidos son:

Up - Indica que el enlace está activado.

Down - Indica que el enlace está desactivado.

Disabled - Indica que el operador ha inhabilitado el enlace.

Not present - Indica que el enlace está configurado, pero hay un problema de hardware.

Secondary Interface and State

Circuito de marcación que se utiliza como seguridad para la interfaz primaria asociada. Los estados válidos son:

Up - Indica que el enlace está activado.

Down - Indica que el enlace está desactivado. Esto también se produce cuando la red base para el secundario está inhabilitado en el indicador `Config>` o en la consola del operador.

Testing - Indica que el enlace está en proceso de establecer una conexión.

Available - Indica que el enlace está en la modalidad de espera.

Configuración de Restauración de WAN

La característica Redireccionamiento de WAN

Este capítulo describe la característica Redireccionamiento de WAN. Incluye las secciones siguientes:

- “Visión general del Redireccionamiento de WAN”
- “Configuración del Redireccionamiento de WAN” en la página 101

Visión general del Redireccionamiento de WAN

El Redireccionamiento de WAN le permite configurar una ruta alternativa de tal manera que, si un enlace primario falla, el direccionador inicia automáticamente una nueva conexión con el destino a través de la ruta alternativa. Consulte “Visión general de Restauración de WAN, Redireccionamiento de WAN y Marcación en desbordamiento” en la página 71 para ver una explicación de la Restauración de WAN y cómo el Redireccionamiento de WAN y la Marcación en desbordamiento trabajan conjuntamente.

El proceso de Redireccionamiento de WAN implica las siguientes acciones:

1. Detección de la anomalía en el enlace primario
2. Conmutación al enlace alternativo
3. Detección de la recuperación del enlace primario
4. Conmutación de vuelta al enlace primario

El enlace primario puede ser cualquier enlace en el que puede configurar protocolos direccionables (por ejemplo, IP o IPX) y no es necesario que el tipo de enlace de datos del enlace alternativo coincida con el tipo de enlace de datos del enlace primario. Por ejemplo, el enlace alternativo puede ser una interfaz LAN, una interfaz serie PPP, Frame Relay o X.25, o un circuito de marcación PPP o Frame Relay. A continuación se incluyen ejemplos de tipos de interfaz que no pueden ser enlaces alternativos: interfaces serie SDLC, interfaces serie SRLY y redes de base como V.25bis y RDSI.

Nota: Si el enlace primario o alternativo es un circuito de marcación, no puede configurarse para marcación bajo demanda. Utilice el mandato **set idle 0** en el indicador `Circuit Config>` para configurar el circuito de marcación de manera que no pueda realizar la marcación bajo demanda. Consulte “Configuring and Monitoring Dial Circuits” en el manual *Nways Multiprotocol Access Services Guía del usuario de software* para obtener más información.

Configuración del Redireccionamiento de WAN

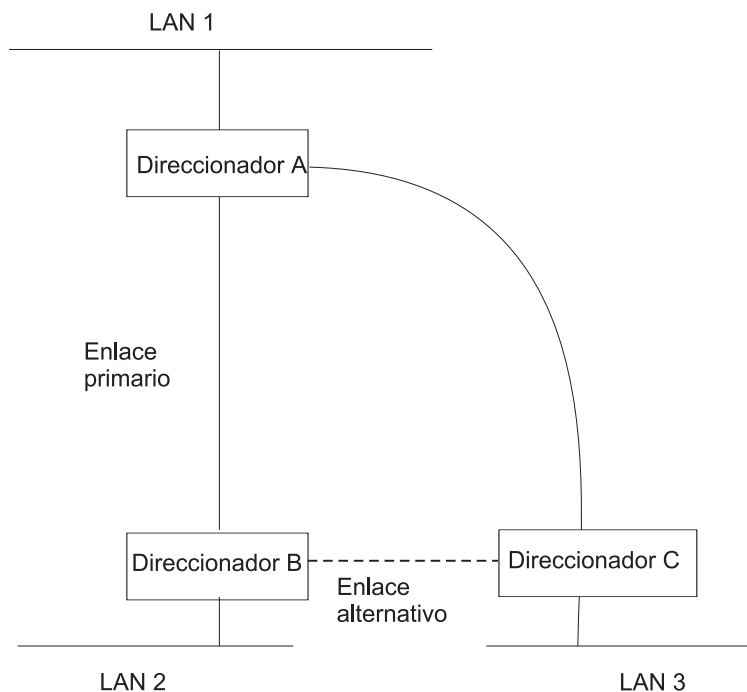


Figura 3. Redireccionamiento de WAN. Normalmente existe una conexión entre los direccionadores A y B y los direccionadores A y C. Si falla el enlace primario entre los direccionadores A y B, el Redireccionamiento de WAN establece un enlace alternativo entre los direccionadores B y C. Entonces, los direccionadores se podrán comunicar a través del direccionador C.

Marcación en desbordamiento

La marcación en desbordamiento le permite utilizar una interfaz alternativa para el tráfico de IP, cuando la velocidad de tráfico en el enlace primario alcance un determinado umbral. Esto quiere decir que no es preciso que la interfaz primaria esté desactivada antes de activar el enlace alternativo. Cuando el tráfico de la interfaz primaria alcanza el umbral especificado, el direccionador activa el enlace alternativo. Para utilizar la marcación en desbordamiento, es preciso configurar el Redireccionamiento de WAN y la interfaz primaria tiene que ser Frame Relay. IP es el único protocolo que puede conmutarse a la interfaz alternativa mediante la marcación en desbordamiento. Además, cuando se utiliza la marcación en desbordamiento se debe utilizar OSPF como protocolo de direccionamiento de IP en lugar de RIP.

Para obtener información acerca de la configuración de la marcación en desbordamiento, consulte "Mandatos de configuración de Restauración de WAN, Redireccionamiento de WAN y Marcación en desbordamiento" en la página 77.

Supervisión de ancho de banda

El intervalo de la supervisión de ancho de banda puede configurarse para la marcación de desbordamiento durante la configuración del Redireccionamiento de WAN. Se supervisa la utilización del ancho de banda de recepción y transmisión de la interfaz primaria. Cuando el ancho de banda de la interfaz primaria alcanza el umbral *add*, se genera una petición de Redireccionamiento de WAN para activar la interfaz alternativa. Si el Redireccionamiento de WAN activa satisfactoriamente la

interfaz alternativa, IP detiene el direccionamiento a través de la interfaz primaria y empieza el direccionamiento a través de la interfaz alternativa.

Si el Redireccionamiento de WAN no consigue activar la ruta alternativa, intentará activar periódicamente la interfaz alternativa hasta que la utilización de ancho de banda de la interfaz primaria sea menor que el umbral *drop*.

Cuando la utilización del ancho de banda de recepción y transmisión de la interfaz primaria alcanza el umbral *drop* y el período de tiempo mínimo de activación configurado ha caducado, se elimina la interfaz alternativa. Esto hace que IP deje de direccionarse a través de la interfaz alternativa y empiece a utilizar la interfaz primaria.

Los valores de umbral *add* y *drop* se especifican como porcentaje de la velocidad de línea configurada para el enlace primario. La velocidad de línea configurada no coincide siempre con la velocidad real del enlace. La cantidad de tráfico en el enlace, en cada dirección, se calcula por separado. El umbral se sobrepasa si el tráfico en cualquier dirección es mayor que el porcentaje especificado.

Configuración del Redireccionamiento de WAN

A continuación se describen los pasos necesarios para configurar el Redireccionamiento de WAN. La sección siguiente muestra un ejemplo sobre cómo realizar estas tareas.

Para configurar el Redireccionamiento de WAN, tiene que realizar las siguientes acciones:

1. Configure el enlace primario.
2. Configure el enlace alternativo.
3. Asigne el enlace alternativo al enlace primario. También puede especificar un período de estabilización para el enlace primario.

Puede especificar un valor de período del día de retorno para el enlace primario que se producirá después de que acabe el período de estabilización (si está configurado). Esto permite que el secundario siga activado hasta el momento que el usuario desee, y que retorne al primario durante las horas de menor actividad.

Nota: Los enlaces primario y alternativo pueden ser tipos de enlace de datos distintos. Los enlaces primario y alternativo pueden ser:

- Una interfaz LAN.
- Una interfaz serie PPP.
- Una interfaz serie Frame Relay.
- Una interfaz serie X.25.
- Un circuito de marcación PPP.
- Un circuito de marcación Frame Relay.

Ejemplo de configuración del Redireccionamiento de WAN

La Figura 4 muestra el redireccionamiento de WAN utilizando un circuito de marcación Frame Relay a través de RDSI como enlace alternativo. Si el DLCI Frame Relay entre el direccionador A y el direccionador C falla, el Redireccionamiento de WAN utiliza el circuito de marcación para establecer una conexión alternativa a través del direccionador D. Si falla uno de los enlaces primarios desde una sucursal a la sede central, el Redireccionamiento de WAN establece una ruta alternativa hacia la sede central a través de otra sucursal.

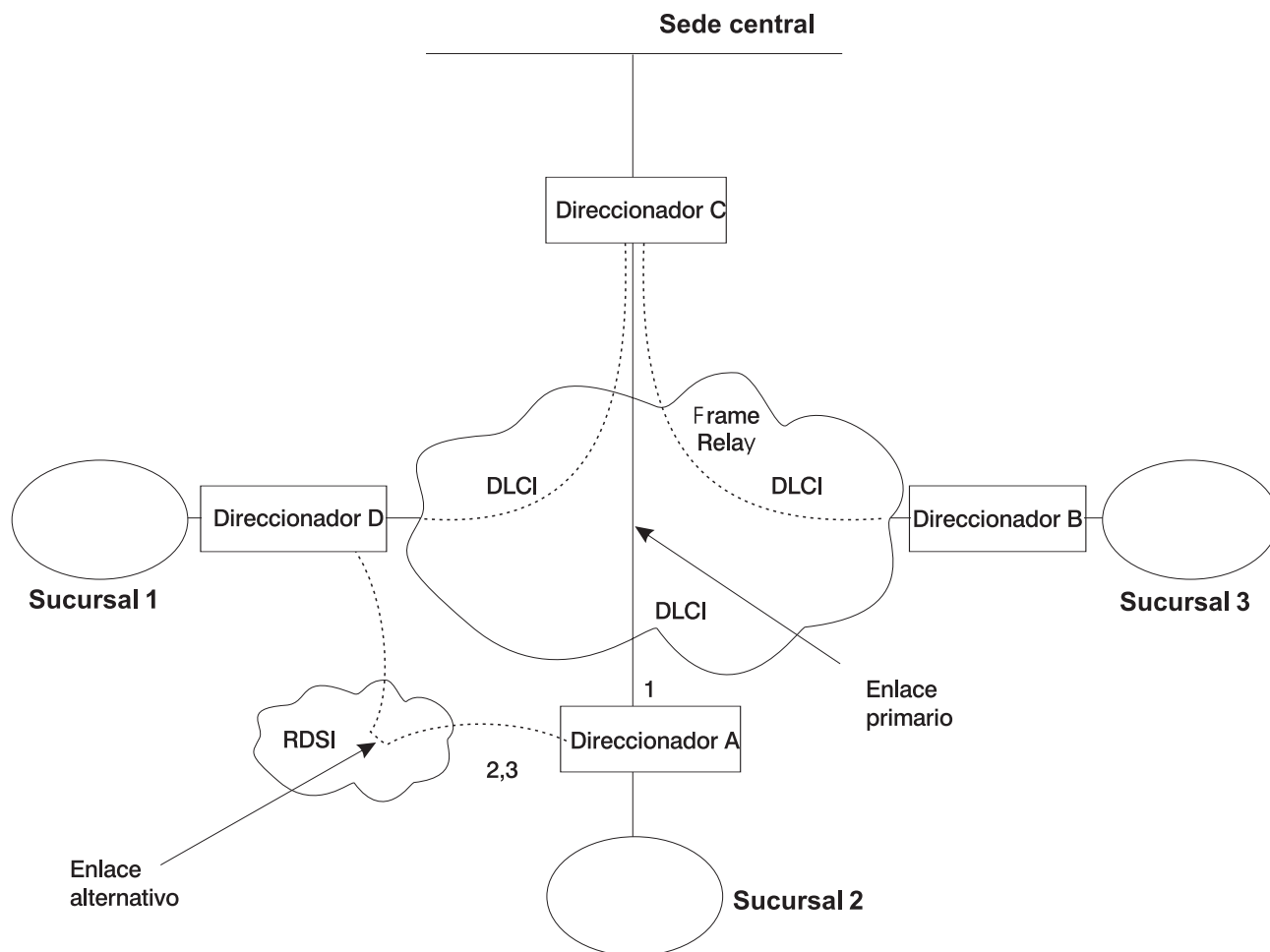


Figura 4. Ejemplo de configuración del Redireccionamiento de WAN. Las sucursales utilizan Frame Relay para conectarse a la sede central.

Las secciones siguientes describen cómo configurar el Redireccionamiento de WAN en el Direccionador A de la Figura 4. Tendrá que realizar lo siguiente:

- Configurar la interfaz Frame Relay primaria (1) para que tenga un PVC o un Grupo PVC necesario, o que habilite la característica que no es PVC en la interfaz Frame Relay.
- Configurar la interfaz RDSI (2) y su circuito de marcación Frame Relay (3).
- Asignar el circuito de marcación para que sea el enlace alternativo para la interfaz Frame Relay primaria, y emitir el mandato `set idle 0` en el indicador de marcación `Circuit Config>` para inhabilitar la marcación bajo demanda para este circuito.

- Opcionalmente, puede asignar:
 - Un período de estabilización para el enlace primario.
 - La ventana del período de día de retorno para el enlace primario.

Estas tareas se describen a continuación con detalle.

Configuración de la interfaz Frame Relay

Para configurar la interfaz Frame Relay para el Redireccionamiento de WAN, en el Direcccionador A, añada un PVC entre los Direcccionadores A y C en la interfaz Frame Relay primaria.

Para conseguir que la interfaz FR primaria se declare desactivada cuando se pierda la conexión con otro(s) direccionador(es), tiene tres opciones:

1. Habilite la característica que no es PVC. Cuando se habilite esta característica, la interfaz FR se desactivará cuando no haya PVC activos.
2. Configure un PVC como sea necesario, pero no incluya el PVC en un grupo de PVC necesario. En este caso, la interfaz FR se desactiva cuando el PVC está inactivo.
3. Configure un conjunto de PVC como sea necesario y como parte de un grupo de PVC necesario. En este caso, la interfaz FR se desactiva cuando todos los PVC de un grupo de PVC necesario están inactivos.

Siga estos pasos para configurar la interfaz Frame Relay primaria:

1. Si no lo ha hecho todavía, defina el enlace de datos en la interfaz RDSI a Frame Relay.

```
Config>set data-link frame relay
Interface Number [0]? 2
```

2. Entre el proceso de configuración de Frame Relay.

```
Config>network
What is the network number [0]?2
Frame Relay user configuration
FR Config>
```

Nota: Complete *uno* solo de los dos pasos restantes para configurar la interfaz Frame Relay primaria.

3. Añada un PVC utilizando el mandato **add permanent-virtual-circuit**.

Para configurar el PVC como necesario (Required):

Entre **y** como respuesta a la pregunta “Is circuit required for interface operation ? (¿Es el circuito necesario para la operación de interfaz?)”.

Para configurar el PVC como miembro de un grupo de PVC necesario:

- a. Entre **y** como respuesta a la pregunta “Does circuit belong to a Required PVC group ? (¿Pertenece el circuito a un grupo de PVC necesario?)”.
- b. Entre un nombre de grupo como respuesta a la pregunta “What is the group name ? (¿Cuál es el nombre de grupo?)”.

Si ya ha añadido los PVC, utilice el mandato **change permanent-virtual-circuit** para configurar el PVC como necesario (Required) y asignarlo como un Grupo de PVC necesario, de la manera más adecuada. Consulte Using Frame Relay Interfaces en el manual *Nways Multiprotocol Access Services Guía del usuario de software* para obtener más información.

Configuración del Redireccionamiento de WAN

```
FR Config>add permanent-virtual-circuit
Circuit number [16]?
Committed Information Rate (CIR) in bps [64000]?
Committed Burst Size (Bc) in bits [64000]?
Excess Burst Size (Be) in bits [0]?
Assign circuit name []?
Is circuit required for interface operation [N]?y
Does the circuit belong to a required PVC group [N]? y
What is the group name []?group1
```

4. Si lo desea, habilite la característica que no es PVC.

Nota: Complete este paso *sólo* si ha saltado el paso anterior.

```
FR Config>enable no-pvc
```

Existen unos parámetros adicionales que se pueden definir para Frame Relay. Para obtener más información, consulte 'Using Frame Relay' en el manual *Nways Multiprotocol Access Services Guía del usuario de software*.

Configuración de la interfaz RDSI y del circuito de marcación

Configure la interfaz RDSI y el circuito de marcación entre el Direccionador A y el Direccionador D. Consulte 'Using the ISDN Interface' en el manual *Nways Multiprotocol Access Services Guía del usuario de software* para obtener información sobre cómo configurar interfaces RDSI y circuitos de marcación.

A diferencia de la Restauración de WAN, debe configurar protocolos direccionables en el circuito de marcación que se utilizarán como enlace alternativo. Si no se puede evitar que estos protocolos direccionables envíen paquetes de mantenimiento, el enlace alternativo establecerá una conexión, aunque el redireccionamiento no sea necesario. En este caso, si sólo desea utilizar el enlace alternativo para el redireccionamiento, inhabilite el circuito de marcación. Para inhabilitar el circuito de marcación, entre el mandato **disable interface** en el indicador `Config>`.

Si tiene varios circuitos de marcación asignados a la interfaz RDSI, puede definir una prioridad para los circuitos de marcación. Si todos los canales B tienen circuitos de marcación activos en la interfaz física y un circuito con una prioridad más alta recibe un paquete, terminará la conexión de prioridad más baja y el circuito de alta prioridad establecerá una conexión.

Puede definir la prioridad entre 0 y 15, donde 15 es el circuito de prioridad más alta, y 0 es el circuito de prioridad más baja. La prioridad por omisión para nuevos circuitos de marcación es 8. Entre **set priority** en el indicador `Circuit Config>` para cambiar la prioridad.

Asignación y configuración del enlace alternativo

Entre el proceso de configuración de redireccionamiento de WAN para asignar el circuito de marcación como enlace alternativo para una interfaz LAN, una interfaz serie PPP, Frame Relay o X.25, o un circuito de marcación PPP o Frame Relay y, si lo desea, especifique los períodos de estabilización y/o la ventana de hora del día de retorno.

Hay tres tipos de períodos de estabilización:

- *First stabilization period* es la cantidad de tiempo que el direccionador espera a que la interfaz primaria se active cuando el direccionador intenta activarla. Si, después del primer período de estabilización, el enlace primario no se ha activado, el redireccionamiento de WAN activará el enlace alternativo.

- *Stabilization period* es la cantidad de tiempo que el direccionador espera para asegurarse de que el enlace primario sea fiable, antes de conmutar de vuelta, desde el enlace alternativo al enlace primario.
- *Routing stabilization period* es la cantidad de tiempo que el direccionador mantiene activos los enlaces primario y alternativo, después de conmutar de vuelta desde el enlace alternativo al enlace primario. Los protocolos de direccionamiento, como OSPF o RIP, utilizan este período de tiempo para reconocer la disponibilidad de la nueva ruta a través del enlace primario, antes de que el enlace alternativo se desactive.

La ventana de hora del día de retorno indica la hora específica del día en que el usuario desea conmutar de vuelta al enlace primario después de su activación y de que haya transcurrido el tiempo de estabilidad configurado.

Con un reloj de 24 horas, el usuario especifica las horas de inicio y de parada de la ventana de retorno. El secundario permanece activado y no se desactiva hasta que se alcanza la hora de inicio. Si la hora del día en que se activa el primario se encuentra entre las horas de inicio y de parada (en la ventana), la conmutación al enlace primario se produce inmediatamente después de llegar a la hora de estabilidad.

Siga estos pasos para asignar y configurar el enlace alternativo:

1. Entre el proceso de configuración de Restauración de WAN.

```
Config>feature wrs
WAN Restoral user configuration
```

2. Asigne el circuito de marcación como enlace alternativo para la interfaz Frame Relay primaria.

```
WRS Config>add alternate-circuit
Alternate interface number [0]? 4
Primary interface number [0]? 1
```

3. Habilite el circuito alternativo.

```
WRS Config>enable alternate-circuit
Alternate interface number [0]? 4
```

4. Opcionalmente, especifique un primer período de estabilización.

Para definir el primer período de estabilización para una interfaz primaria específica, utilice el mandato **set first-stabilization-period**. Para definir un primer período de estabilización por omisión para todas las interfaces que no tienen definidos períodos específicos, utilice el mandato **set default first-stabilization-period**.

```
WRS Config>set first-stabilization-period
Primary interface number [0]?
First primary stabilization time (0 - 3600 seconds -1=default) [-1]?
```

```
WRS Config>set default first-stabilization-period
Default first primary stabilization time (0 - 3600 seconds) [0]?
```

5. Opcionalmente, especifique un período de estabilización. Para definir un período de estabilización para interfaces específicas, utilice el mandato **set stabilization-period**. Para definir un período de estabilización por omisión para todas las interfaces que no tienen definidos períodos específicos, utilice el mandato **set default stabilization-period**.

```
WRS Config>set stabilization-period
Primary interface number [0]?
First primary stabilization time (0 - 3600 seconds -1=default) [-1]?
WRS Config>set default stabilization-period
Default first primary stabilization time (0 - 3600 seconds) [0]?
```

Configuración del Redireccionamiento de WAN

- Opcionalmente, especifique un período de estabilización de direccionamiento. Para definir un período de estabilización de direccionamiento para interfaces específicas, utilice el mandato **set routing-stabilization**.

```
WRS Config>set routing-stabilization
Primary interface number [0]? 1
Routing stabilization time (0 - 3600 seconds) [15]?
```

- Opcionalmente, especifique una ventana de hora del día de retorno.

Para definir las horas de inicio y parada para ventanas de interfaz específicas, utilice los mandatos **start-time-of-day-revert-back** y **stop-time-of-day-revert-back**. El valor por omisión, cero, quiere decir que no se configura ninguna ventana. El reloj de 24 horas comienza a la 1 a.m. y finaliza a las 24 horas (medianoche). Si las horas de inicio y parada son la misma (pero distinta de cero), el retorno se producirá exactamente a esa hora.

A continuación se muestran dos ejemplos de definición de la ventana de retorno:

- La hora de inicio 23 y la hora de parada 3 crearán una ventana de retorno desde la 11 p.m. a las 3 a.m.
- La hora de inicio 1 y la hora de parada 5 crearán una ventana de retorno desde la 1 a.m. a las 5 a.m.

```
WRS Config> set start-time-of-day-revert-back
Primary interface number [0]?
Time-of-Day revert back window start (1 - 24 hours, 0 = not configured) [0]?
WRS Config> set stop-time-of-day-revert-back
Primary interface number [0]?
Time-of-Day revert back window stop (1 - 24 hours, 0 = not configured) [0]?
```

Utilización de la característica Network Dispatcher

Este capítulo describe cómo utilizar la característica Network Dispatcher y contiene las secciones siguientes:

- “Visión general de Network Dispatcher”
- “Equilibrio del tráfico TCP y UDP mediante Network Dispatcher” en la página 108
- “Alta disponibilidad para Network Dispatcher” en la página 109
- “Configuración de Network Dispatcher” en la página 111
- “Utilización de Network Dispatcher con el servidor TN3270” en la página 119
- “Utilización de Network Dispatcher con la Antememoria del servidor de la web” en la página 121
- “Utilización de Network Dispatcher con la Antememoria de eNetwork Host On-Demand Client” en la página 121
- “Utilización de Network Dispatcher con la Antememoria escalable de alta disponibilidad (SHAC)” en la página 121

Network Dispatcher utiliza la tecnología de equilibrio de carga de la IBM Research Division para determinar cuál es el servidor más adecuado para recibir cada conexión nueva. Es la misma tecnología utilizada en el producto eNetwork Dispatcher de IBM para Solaris, Windows NT y AIX.

Visión general de Network Dispatcher

Network Dispatcher es una característica que mejora espectacularmente el rendimiento de los servidores reenviando peticiones de sesiones TCP/IP a distintos servidores en un grupo de servidores, equilibrando así la carga de las peticiones entre todos los servidores. Este reenvío es transparente para los usuarios y para las aplicaciones. Network Dispatcher es útil para aplicaciones de servidor, tales como el correo electrónico, los servidores World Wide Web, las consultas de bases de datos paralelas distribuidas y otras aplicaciones TCP/IP.

Network Dispatcher puede utilizarse también para establecer el equilibrio de carga del tráfico de aplicaciones UDP sin estado en un grupo de servidores.

Network Dispatcher puede ayudar a maximizar el potencial de su sitio proporcionando una solución potente, flexible y escalable para problemas derivados de picos en la demanda. Durante los períodos en que se producen picos en la demanda, Network Dispatcher puede encontrar automáticamente el servidor óptimo para gestionar las peticiones entrantes.

La función Network Dispatcher no utiliza un servidor de nombres de dominio para el equilibrio de carga. Equilibra el tráfico entre los servidores mediante una combinación exclusiva de equilibrio de carga y software de gestión. Network Dispatcher puede detectar también un servidor anómalo y reenviar el tráfico a otros servidores disponibles.

Todas las peticiones de clientes enviadas a la máquina donde se halla Network Dispatcher se reenvían al servidor seleccionado por Network Dispatcher como servidor óptimo, según unos pesos determinados que se han definido de manera dinámica. Puede utilizar los valores por omisión para estos pesos, o bien cambiar los valores durante el proceso de configuración.

El servidor devuelve una respuesta al cliente sin que Network Dispatcher se vea involucrado. No se necesita software adicional en los servidores para establecer comunicación con Network Dispatcher.

La función Network Dispatcher es la clave para la gestión estable y eficiente de una red grande y escalable de servidores. Con Network Dispatcher, podrá enlazar muchos servidores individuales en lo que parecerá ser un único servidor virtual. Así, su sitio aparecerá ante el mundo como una única dirección IP. Network Dispatcher funciona de forma independiente de un servidor de nombres de dominio; todas las peticiones se envían a la dirección IP de la máquina que contiene Network Dispatcher.

Network Dispatcher permite que una aplicación de gestión basada en SNMP supervise el estado de Network Dispatcher recibiendo estadísticas básicas y situaciones potenciales de alerta. Consulte "SNMP Management" en el manual *Consulta de configuración y supervisión de protocolos Volumen 1* para obtener más información.

Network Dispatcher aporta claras ventajas para el tráfico de equilibrio de carga hacia los servidores agrupados en clusters, que producen una gestión estable y eficiente de su sitio.

Equilibrio del tráfico TCP y UDP mediante Network Dispatcher

Hay muchos enfoques distintos para el equilibrio de carga. Algunos de estos enfoques permiten a los usuarios elegir un servidor diferente al azar si el primer servidor es lento o no responde. Otro enfoque es el rotatorio, en el que el servidor de nombres de dominio selecciona un servidor para gestionar las peticiones. Este enfoque es mejor, pero no tiene en cuenta la carga actual en el servidor de destino, ni siquiera si el servidor de destino está disponible.

Network Dispatcher puede realizar el equilibrio de carga de las peticiones en diferentes servidores según el tipo de petición, un análisis de la carga en los servidores o un conjunto configurable de pesos que el usuario debe asignar. Para gestionar cada tipo distinto de equilibrio, Network Dispatcher tiene los siguientes componentes:

Ejecutor Equilibra la carga de las conexiones basadas en el tipo de petición recibida. Los tipos de petición más habituales son HTTP, FTP y Telnet. Este componente siempre está en ejecución.

Consejeros Consultan los servidores y analizan los resultados por protocolo para cada servidor. El consejero pasa esta información al **gestor** para que defina el peso adecuado. El consejero es un componente opcional.

Network Dispatcher da soporte a consejeros para FTP, HTTP, SMTP, NNTP, POP3 y Telnet, así como a un consejero TN3270 que trabaja con servidores TN3270 en los IBM 2210, IBM 2212 y IBM 2216, y a un consejero MVS que trabaja con Workload Manager (WLM) en los sistemas MVS. WLM gestiona la cantidad de carga de trabajo en un ID MVS individual. Network Dispatcher puede utilizar WLM como ayuda para el equilibrio de carga de las peticiones en los servidores MVS que ejecutan OS/390 V1R3 o un release posterior.

No hay consejeros de protocolo específicos para los protocolos UDP. Si tiene servidores MVS, puede utilizar el consejero del sistema MVS para proporcionar información sobre la carga de los servidores. Además, si el puerto gestiona tráfico TCP y UDP, puede utilizarse el consejero del protocolo TCP adecuado para proporcionar la entrada del consejero para el puerto. Network Dispatcher utilizará esta entrada en el equilibrio de carga del tráfico TCP y UDP en ese puerto.

Gestor

Define los pesos para un servidor basándose en los elementos siguientes:

- Contadores internos en el ejecutor
- Retroalimentación de los servidores, proporcionada por los consejeros de protocolo
- Retroalimentación de un supervisor del sistema (consejero MVS).

El gestor es un componente opcional. No obstante, si no utiliza el gestor, Network Dispatcher realizará el equilibrio de carga mediante un método de planificación rotatorio, basado en los pesos de servidor actuales.

Al utilizar Network Dispatcher para establecer el equilibrio de carga del tráfico UDP sin estado, sólo debe utilizar los servidores que respondan al cliente mediante la dirección IP de destino de la petición. Consulte "Configuración de un servidor para Network Dispatcher" en la página 117 para obtener una explicación más completa.

Alta disponibilidad para Network Dispatcher

La función Network Dispatcher básica tiene las siguientes características, que la convierten en un punto único de anomalía desde muchas perspectivas distintas:

- Examina todo el tráfico que entra. Si algunos paquetes de una conexión existente utilizan una vía de acceso diferente a través de un Network Dispatcher distinto para llegar a un servidor, éste restablece la conexión de inmediato.
- Hace un seguimiento de todas las conexiones establecidas y, aunque no las termine, las entradas perdidas de la tabla de conexiones de Network Dispatcher darán como resultado el restablecimiento de la conexión.
- Para cualquier direccionador de saltos anterior, aparece como el último salto y la terminación de la conexión.

Todas estas características hacen que las siguientes anomalías sean críticas para todo el cluster:

- Si Network Dispatcher falla por alguna razón, se perderán todas las tablas de conexión y, por consiguiente, se perderán también todas las conexiones existentes del cliente al servidor. Suponiendo que exista un segundo Network Dispatcher que pueda dirigir un cliente a los servidores, las nuevas conexiones sólo podrán pasar los retardos de protocolo de direccionamiento habituales, que pueden ser de varios minutos.
- Si la interfaz de Network Dispatcher configurada con el direccionador IP anterior tiene una anomalía, debe haber otra interfaz para obtener el mismo Network Dispatcher, en cuyo caso el direccionador IP realiza la recuperación

Utilización de Network Dispatcher

(mediante el mecanismo de caducidad ARP, con retardos del orden de varios minutos), o se perderán todas las conexiones.

- Si la interfaz de Network Dispatcher con los servidores tiene una anomalía, el direccionador de saltos anterior supone que Network Dispatcher es el último salto y, por consiguiente, no redireccionará las nuevas conexiones. Las conexiones existentes se perderán y no se establecerán nuevas conexiones.

En todos estos casos de anomalías, que no sólo son anomalías de Network Dispatcher, sino también anomalías de los elementos próximos a Network Dispatcher, se perderán todas las conexiones existentes. Incluso con un Network Dispatcher de copia de seguridad que ejecute mecanismos estándar de recuperación de IP, la recuperación es lenta, incluso en el mejor de los casos, y se aplica solamente a las nuevas conexiones. En el peor de los casos, no se produce la recuperación de las conexiones.

Para mejorar la disponibilidad de Network Dispatcher, la función de Alta Disponibilidad de Network Dispatcher utiliza los siguientes mecanismos:

- Dos Network Dispatchers con conectividad con los mismos clientes y el mismo cluster de servidores, así como conectividad entre los Network Dispatchers.
- Un mecanismo “Heartbeat” entre ambos Network Dispatchers para detectar una anomalía de Network Dispatcher.
- Un criterio de capacidad de alcance, para identificar qué sistema principal puede alcanzarse o no desde cada Network Dispatcher.
- La sincronización de las bases de datos de Network Dispatcher (es decir, las tablas de conexiones, las tablas de capacidad de alcance y otras bases de datos).
- La lógica para elegir el Network Dispatcher activo, que está a cargo de un cluster de servidores determinado, y el Network Dispatcher de espera, que se sincroniza continuamente para ese cluster de servidores.
- Un mecanismo para realizar una entrada en función IP rápida, cuando la lógica o un operador decide conmutar entre el estado activo y de espera.

Detección de anomalías

Junto al criterio básico de la detección de anomalías (la pérdida de conectividad entre los Network Dispatchers activo y de espera, detectada mediante los mensajes Heartbeat), existe otro mecanismo de detección de anomalías, denominado “criterio de capacidad de alcance”. Al configurar Network Dispatcher, se proporciona una lista de sistemas principales que cada Network Dispatcher debe ser capaz de alcanzar para trabajar de manera correcta. Los sistemas principales pueden ser direccionadores, servidores IP u otros tipos de sistemas principales. La capacidad de alcance de un sistema principal se obtiene realizando PING en el sistema principal.

La conmutación se realiza si los mensajes Heartbeat no pueden llegar, o si el Network Dispatcher activo deja de cumplir el criterio de capacidad de alcance y se puede alcanzar el Network Dispatcher de espera. Para tomar la decisión basada en toda la información disponible, el Network Dispatcher activo envía regularmente sus posibilidades de alcance al Network Dispatcher de espera. Entonces, el Network Dispatcher de espera compara las posibilidades con las suyas propias y decide si realiza la conmutación.

Sincronización de bases de datos

Los Network Dispatchers primario y de copia de seguridad mantienen sincronizadas sus bases de datos mediante el mecanismo "Heartbeat". La base de datos de Network Dispatcher incluye tablas de conexión, tablas de capacidad de alcance y otros tipos de información. La función de Alta disponibilidad de Network Dispatcher utiliza un protocolo de sincronización de bases de datos que asegura que ambos Network Dispatchers contengan las mismas entradas de tabla de conexión. Esta sincronización tiene en cuenta un margen de error conocido para retardos de la transmisión. El protocolo realiza una sincronización inicial de bases de datos y después mantiene la sincronización de bases de datos a través de actualizaciones periódicas.

Estrategia de recuperación

En caso de una anomalía en Network Dispatcher, el mecanismo de entrada en función de IP dirigirá de inmediato todo el tráfico hacia el Network Dispatcher de espera. El mecanismo de Sincronización de bases de datos asegura que el Network Dispatcher de espera tiene las mismas entradas que el activo. Cuando se produzca la anomalía en la red (cualquier fragmento intermedio de hardware o software entre el cliente y el servidor de fondo), y existe una vía de acceso alternativa a través del Network Dispatcher de espera que trabaja, la conmutación se realiza a través de la vía de acceso alternativa.

Entrada en función de IP

Nota: Se supone que las Direcciones IP de cluster se encuentran en la misma subred lógica que el direccionador de salto (direccionador IP) anterior.

El Direccionador de IP resolverá la dirección de cluster a través del protocolo ARP. Para realizar la entrada en función de IP, el Network Dispatcher (de espera que pasa a estar activo) emitirá una petición ARP a sí mismo, que se emitirá a todas las redes conectadas directamente que pertenezcan a la subred lógica del cluster. El direccionador IP de los saltos anteriores actualizará sus tablas ARP (según el documento RFC826) para enviar todo el tráfico para ese cluster al nuevo Network Dispatcher activo (que antes estaba de espera).

Configuración de Network Dispatcher

Hay muchas maneras de configurar Network Dispatcher para dar soporte a su sitio. Si sólo tiene un nombre de sistema principal para el sitio al que puedan conectarse todos los clientes, puede definir un único cluster y los puertos a las que desea recibir las conexiones. Esta configuración se muestra en la Figura 5 en la página 112.

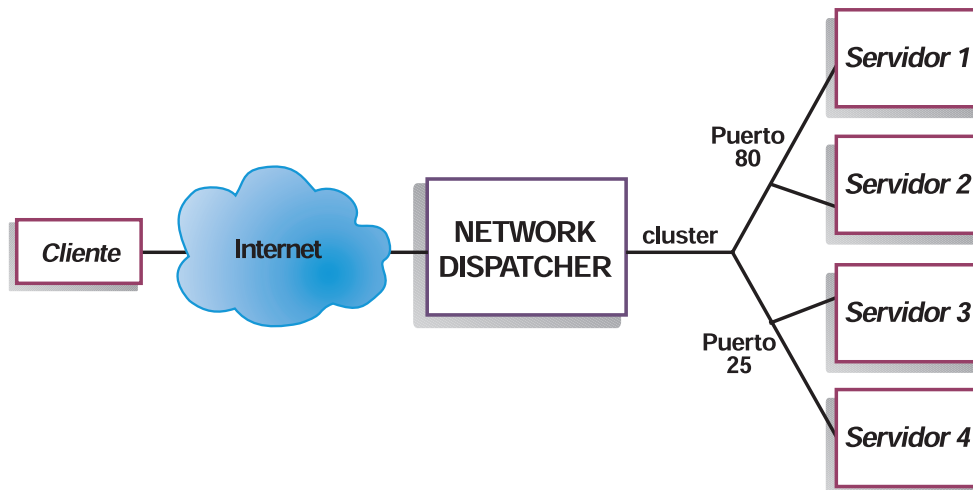


Figura 5. Ejemplo de Network Dispatcher configurado con un único cluster y 2 puertos

Se necesitaría otra manera de configurar Network Dispatcher si el sitio contuviera los sistemas principales de varias compañías o departamentos y cada uno de ellos hubiera llegado a su sitio con un URL distinto. En este caso, tal vez desee definir un cluster para cada compañía o departamento, así como las puertos en las que desea recibir las conexiones con ese URL, tal como se muestra en la Figura 6 en la página 113.

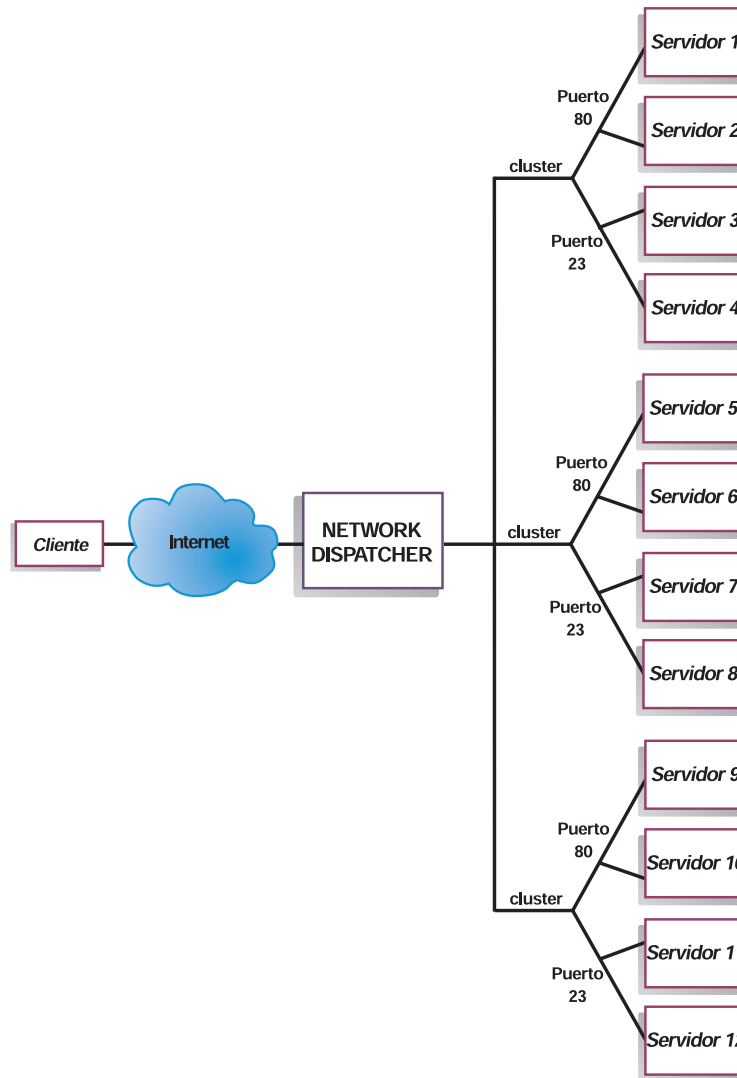


Figura 6. Ejemplo de Network Dispatcher configurado con 3 clusters y 3 URL

Sería adecuada una tercera manera de configurar Network Dispatcher si tuviera un sitio muy grande, con muchos servidores dedicados a cada protocolo soportado. Por ejemplo, podría optar por tener servidores FTP distintos con líneas T3 directas para archivos grandes que pueden bajarse. En este caso, tal vez desee definir un cluster para cada protocolo, con un solo puerto pero con muchos servidores, tal como se muestra en la Figura 7 en la página 114.

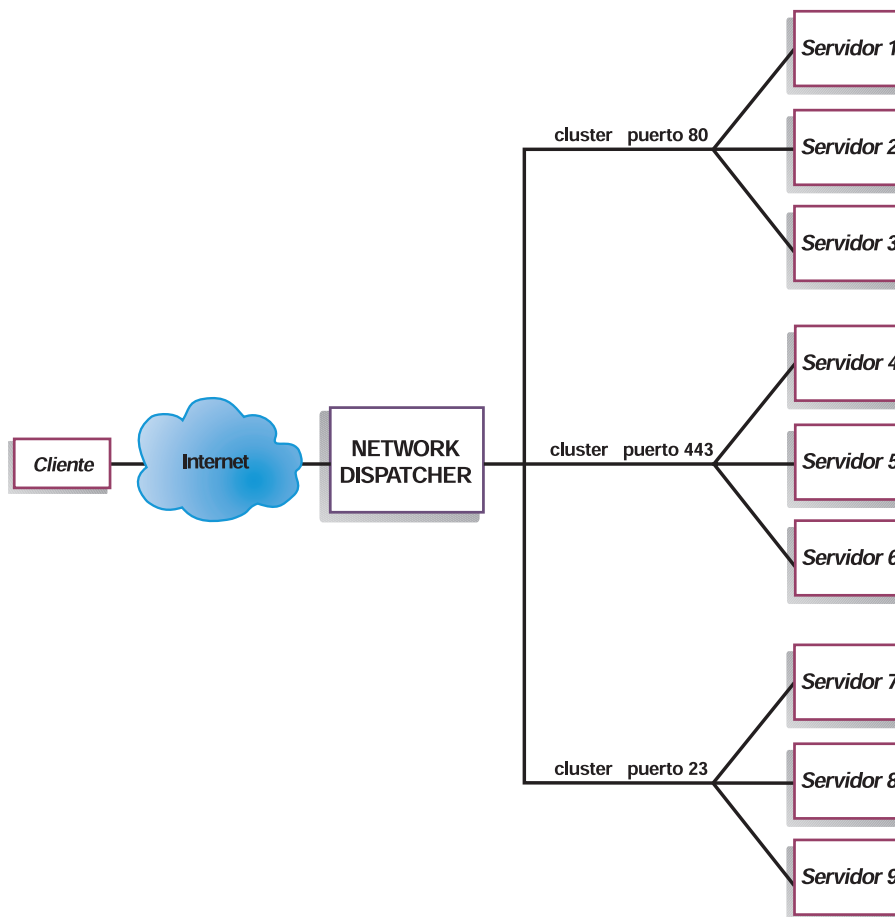


Figura 7. Ejemplo de Network Dispatcher configurado con 3 clusters y 3 puertos

Pasos de la configuración

Antes de configurar Network Dispatcher:

1. Asegúrese de que Network Dispatcher tiene interfaces directas con los servidores. Los servidores pueden tener conexiones independientes con el direccionador de la empresa o con Internet, de tal manera que el tráfico de salida desde los servidores a los clientes puede ignorar el Network Dispatcher; no obstante, no tiene que configurar la conexión independiente.

Si la alta disponibilidad es importante para la red, una configuración típica de alta disponibilidad se muestra en la Figura 8 en la página 115.

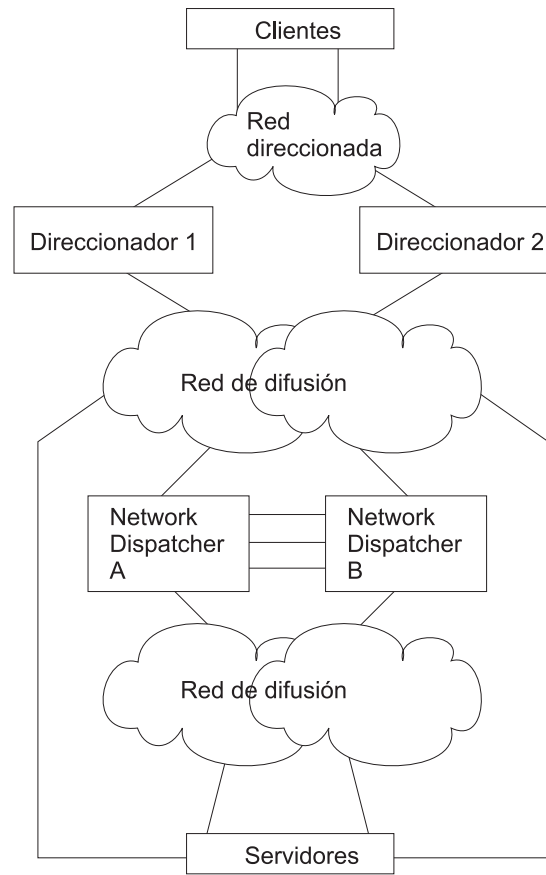


Figura 8. Configuración de Network Dispatcher de alta disponibilidad

2. Configure las interfaces del dispositivo. Esto incluye la configuración de todas las interfaces, las direcciones IP en todas las interfaces y cualquier protocolo de direccionamiento aplicable. Network Dispatcher utiliza la dirección IP interna del direccionador, de manera que también debe configurarse utilizando el mandato `set internal-ip-address`. La dirección IP interna no debe coincidir con una dirección de cluster configurada en Network Dispatcher. Consulte el capítulo *Configuring and Monitoring IP* en *Consulta de configuración y supervisión de protocolos Volumen 1* para obtener más información acerca del mandato **set internal-ip-address**.
3. Rearranque o reinicie el dispositivo.

Configuración de Network Dispatcher en un IBM 2216

Para configurar Network Dispatcher en un IBM 2216:

1. Acceda a la característica Network Dispatcher, utilizando el mandato **feature ndr**.
2. Habilite el ejecutor y el gestor utilizando los mandatos **enable executor** y **enable manager**.
3. Configure los clusters utilizando el mandato `add cluster`. Network Dispatcher no anuncia específicamente las direcciones de cluster, de manera que deben seleccionarse las direcciones de cluster que formen parte de una subred anunciada que sea local respecto al direccionador de Network Dispatcher. Habitualmente, esto sería la subred en la que Network Dispatcher recibe el tráfico de cliente desde el siguiente direccionador de salto.

Nota: Las Direcciones IP de cluster no deben coincidir con la dirección IP interna del direccionador y no debe coincidir con ninguna dirección IP de interfaz definida en el direccionador.

4. Configure los puertos de destino TCP y UDP utilizando el mandato **add port** para cada cluster de servidores que servirán el protocolo correspondiente. Los ejemplos de los puertos son: 80 para HTTP, 20 y 21 para FTP y 23 para Telnet.
5. Configure los servidores utilizando los mandatos **add server**. Un servidor siempre se asocia a un puerto y un cluster. Un servidor puede servir a más de un puerto, se puede servir a un puerto en más de un servidor, y un servidor puede pertenecer a más de un cluster, si el sistema operativo del servidor da soporte a múltiples alias.
6. Configure los consejeros utilizando el mandato **add advisor**.

Notas:

- a. Para el consejero MVS, no defina el valor Port Number (valor por omisión = 10007) bajo ningún cluster. Sólo el consejero MVS utiliza este número de puerto para comunicar con WLM en los sistemas MVS.
 - b. Para el consejero TN3270, se entran dos valores de puerto. Es preciso definir el valor de Port Number utilizado para la comunicación cliente-servidor (valor por omisión = 23) bajo los clusters adecuados. No defina el valor de Communication Port (valor por omisión = 10008) bajo ningún cluster. Sólo el consejero TN3270 utiliza el valor de Communication Port para reunir información de carga de los servidores TN3270.
7. Habilite los consejeros que ha configurado utilizando el mandato **enable advisor**.

Si configura Network Dispatcher para alta disponibilidad, continúe con los siguientes pasos. De lo contrario, habrá completado la configuración.

Nota: Realice estos pasos en el Network Dispatcher primario y, a continuación, en la copia de seguridad. Para asegurar la sincronización de bases de datos adecuada, es preciso habilitar el ejecutor del Network Dispatcher primario antes que el ejecutor de la copia de seguridad.

8. Configure si este Network Dispatcher es primario o de copia de seguridad y si la conmutación es manual o automática utilizando el mandato **add backup**.
9. Configure todas las vías en las que se va a realizar el heartbeat entre los Network Dispatchers primario y de copia de seguridad utilizando el mandato **add heartbeat**. Las direcciones IP de origen y de destino especifican una vía. La configuración de más de una vía de acceso de heartbeat entre los Network Dispatchers primario y de copia de seguridad es muy recomendable, para asegurar que la anomalía de una única interfaz no alterará la comunicación de heartbeat entre las máquinas primaria y de copia de seguridad.
10. Configure la lista de las direcciones IP de sistema principal que el Network Dispatcher debe poder alcanzar, para asegurar el pleno servicio, utilizando el mandato **add reach**. Normalmente, será un subconjunto de servidores, el direccionador de empresa o una estación de administración.

Puede cambiar la configuración utilizando los mandatos **set**, **remove** y **disable**. Consulte “Configuración y supervisión de la característica Network Dispatcher” en la página 125 para obtener más información acerca de estos mandatos.

Configuración de un servidor para Network Dispatcher

Para configurar un servidor para su utilización con Network Dispatcher:

1. Establezca un alias para el dispositivo de bucle de retorno.

Para que funcionen los servidores TCP y UDP, debe definir (o preferiblemente establecer un alias) el dispositivo de bucle de retorno (habitualmente denominado **lo0**) en la dirección de cluster. Network Dispatcher no modifica la dirección IP de destino en el paquete IP antes de reenviar el paquete a una máquina servidora. Cuando defina o establezca un alias para el dispositivo de bucle de retorno en la dirección de cluster, la máquina servidora aceptará un paquete que iba dirigido a la dirección del cluster.

Es importante que el servidor utilice la dirección de cluster, en lugar de su propia dirección IP, para responder al cliente. Esto no es un problema con los servidores TCP, pero algunos servidores UDP utilizan su propia dirección IP cuando responden a peticiones enviadas a la dirección de cluster. Cuando el servidor utiliza su propia dirección IP, algunos clientes descartarán la respuesta del servidor, porque no procede de una dirección IP de origen esperada. Sólo debe utilizar servidores UDP que utilicen la dirección IP de destino de la petición cuando respondan al cliente. En este caso, la dirección IP de destino de la petición es la dirección del cluster.

Si tiene un sistema operativo que dé soporte a los alias de interfaz de red, como AIX, Solaris o Windows NT, debe establecer el alias del dispositivo de bucle de retorno en la dirección de cluster. La ventaja de utilizar un sistema operativo que dé soporte a los alias es que puede configurar las máquinas servidoras para que sirvan a varias direcciones de cluster.

Si tiene un servidor con un sistema operativo que no dé soporte a los alias, como HP-UX y OS/2, debe definir **lo0** como la dirección de cluster.

Si el servidor es un sistema MVS que ejecuta TCP/IP V3R2, debe definir la dirección VIPA como la dirección de cluster. Funcionará como una dirección de bucle de retorno. La dirección VIPA no debe pertenecer a una subred que esté conectada directamente con el nodo MVS. Si el sistema MVS ejecuta TCP/IP V3R3, debe definir el dispositivo de bucle de retorno como la dirección de cluster. Si utiliza la alta disponibilidad, debe habilitar RouteD en el sistema MVS, de manera que el mecanismo de entrada en función de alta disponibilidad funcione de manera correcta.

Nota: Los mandatos listados en este capítulo se han probado en los siguientes sistemas operativos y niveles: AIX 4.1.5 y 4.2, HP-UX 10.2.0, Linux, OS/2 Warp Connect Versión 3.0, OS/2 Warp Versión 4.0, Solaris 2.5 (Sun OS 5.5) y Windows NT 3.51 y 4.0.

Utilice el mandato correspondiente a su sistema operativo, tal como se muestra en la Tabla 11 en la página 118, para definir o establecer el alias del dispositivo de bucle de retorno.

Tabla 11. Mandatos para establecer el alias del dispositivo de bucle de retorno (lo0) para Dispatcher

Sistema	Mandato
AIX	ifconfig lo0 alias dirección_cluster
HP-UX	ifconfig lo0 dirección_cluster
Linux	ifconfig lo:1 cluster_address netmask up
OS/2	ifconfig lo cluster_address
Solaris	ifconfig lo0:1 cluster_address 127.0.0.1 up
Windows NT	<ol style="list-style-type: none"> 1. Pulse el botón del ratón sobre Inicio y después sobre Configuración. 2. Pulse el botón sobre Panel de control y, a continuación, efectúe una doble pulsación sobre Red. 3. Si no lo ha hecho todavía, añada el controlador MS Loopback Adapter. <ol style="list-style-type: none"> a. En la ventana Red, pulse el botón sobre Adaptadores. b. Seleccione MS Loopback Adapter y pulse el botón sobre Aceptar. c. Cuando se le solicite, inserte el CD o los discos de instalación. d. En la ventana Red, pulse el botón sobre Protocolos. e. Seleccione Protocolo TCP/IP y pulse el botón sobre Propiedades. f. Seleccione MS Loopback Adapter y pulse el botón sobre Aceptar. 4. Defina la dirección de bucle de retorno como dirección de cluster. Acepte la máscara de subred por omisión (255.0.0.0) y no entre una dirección de pasarela. <p>Nota: Tal vez tenga que salir y volver a entrar en Configuración de red antes de que el controlador MS Loopback aparezca en Configuración de TCP/IP.</p>

2. Compruebe si hay una ruta extra.

En algunos sistemas operativos, es posible que se haya creado una ruta por omisión que se tiene que eliminar.

- a. Compruebe si hay una ruta extra en Windows NT con el siguiente mandato: **route print**
- b. Compruebe si hay una ruta extra en todos los sistemas UNIX y OS/2 con el siguiente mandato: **netstat -nr**
- c. Ejemplo de Windows NT: después de entrar la impresión de ruta, se visualizará una tabla similar a la siguiente. (Este ejemplo muestra cómo se encuentra y se elimina una ruta extra en el cluster 9.67.133.158 con la máscara de red por omisión 255.0.0.0.)

```
Active Routes:
Network Address      Netmask  Gateway Address      Interface  Metric
0.0.0.0             0.0.0.0   9.67.128.1          9.67.133.67  1
9.0.0.0             255.0.0.0 9.67.133.158        9.67.133.158  1
9.67.128.0          255.255.248.0 9.67.133.67         9.67.133.67  1
9.67.133.67         255.255.255.255 127.0.0.1           127.0.0.1    1
9.67.133.158        255.255.255.255 127.0.0.1           127.0.0.1    1
9.255.255.255       255.255.255.255 9.67.133.67         9.67.133.67  1
127.0.0.0           255.0.0.0   127.0.0.1           127.0.0.1    1
224.0.0.0           224.0.0.0   9.67.133.158        9.67.133.158  1
224.0.0.0           224.0.0.0   9.67.133.67         9.67.133.67  1
255.255.255.255     255.255.255.255 9.67.133.67         9.67.133.67  1
```

d. Busque su dirección de cluster en la columna "Gateway Address" (Dirección de pasarela). Si tiene una ruta extra, la dirección de cluster aparece dos veces. En el ejemplo proporcionado, la dirección de cluster (9.67.133.158) aparece en las filas 2 y 8.

e. Busque la dirección de red en cada fila en la que aparece la dirección de cluster. Necesita una de estas rutas y tendrá que suprimir la otra, que es superflua. La ruta extra que se debe suprimir será aquella cuya dirección de red empiece por el primer dígito de la dirección de cluster, seguido de tres ceros. En el ejemplo indicado, la ruta extra es el 1 que aparece en la fila dos, que tiene la dirección de red 9.0.0.0:

```
9.0.0.0      255.0.0.0   9.67.133.158   9.67.133.158   1
```

3. Suprima las rutas extra.

Utilice el mandato de la Tabla 12 para que el sistema operativo suprima las rutas extra.

Tabla 12. Mandatos para suprimir rutas para diversos sistemas operativos	
Sistema operativo	Mandato
AIX	route delete -net <i>dirección_red</i> <i>dirección_cluster</i>
HP-Unix	route delete <i>dirección_cluster</i> <i>dirección_cluster</i>
Solaris	No es necesario suprimir la ruta.
OS/2	No es necesario suprimir la ruta.
Windows NT	route delete <i>dirección_red</i> <i>dirección_cluster</i> Nota: Este mandato se debe entrar en un indicador de MS-DOS.

Utilización de Network Dispatcher con el servidor TN3270

Se puede utilizar Network Dispatcher con un cluster de 2210, 2212, Network Utilities o 2216 que ejecuta la función de servidor TN3270 para proporcionar soporte de servidor TN3270E para entornos 3270 grandes. El consejero TN3270 permite que Network Dispatcher reúna las estadísticas de carga de cada servidor TN3270E en tiempo real para conseguir la mejor distribución posible entre los servidores TN3270. Además de los servidores TN3270 externos al direccionador de Network Dispatcher, uno de los servidores TN3270 del cluster puede ser interno: se puede ejecutar en el mismo direccionador que Network Dispatcher.

Claves para la configuración

La configuración de los servidores TN3270E es esencialmente la misma, tanto si tiene un Network Dispatcher frente a los servidores como si no. De hecho, el servidor TN3270E no sabe que el tráfico de los clientes se está dirigiendo a través de otra máquina. No obstante, hay algunos puntos que deben tenerse en cuenta al configurar los servidores TN3270 externos para su uso con Network Dispatcher:

- Dado que Network Dispatcher no altera la dirección IP de destino en los paquetes (es decir, la dirección de cluster) que reenvía a los servidores, la dirección IP del servidor TN3270 en cada servidor se debe definir de igual manera que la dirección IP del cluster.
- Los direccionadores que ejecutan la función de servidor TN3270 deben conocer la dirección IP de la función TN3270 que se ejecuta en el direccionador para entregar los paquetes a la función de servidor. Por consiguiente, la dirección IP del servidor TN3270 (es decir, la dirección de cluster) debe definirse también en cada direccionador de servidor TN3270 como la dirección IP interna del direccionador, o como dirección secundaria en una de las interfaces del direccionador.
- Debe asegurarse de que los protocolos de direccionamiento que se utilicen en los servidores TN3270E (por ejemplo, OSPF o RIP) no anunciarán la dirección de cluster. El direccionador de Network Dispatcher debe ser "propietario" de la dirección de cluster, por lo que respecta a la red cliente. Network Dispatcher no anuncia específicamente las direcciones de cluster, pero se deben seleccionar las direcciones de cluster que forman parte de una subred anunciada que es local respecto al direccionador de Network Dispatcher.
- Si el tráfico desde el cliente a Network Dispatcher fluye por la misma LAN que el tráfico de Network Dispatcher al servidor, deberá asegurarse de que los servidores no respondan a ARP buscando la dirección de cluster, ya que la dirección de cluster no puede definirse en la interfaz del servidor con esta LAN. Network Dispatcher debe ser el único que responda a ARP en la LAN en la que recibe tráfico de clientes. De manera alternativa, la dirección de cluster puede configurarse en el servidor TN3270 como una dirección de interfaz en otra interfaz, o puede configurarse como dirección IP interna del servidor TN3270.
- Es preciso configurar cada servidor TN3270 en Network Dispatcher con una dirección IP de servidor exclusiva. También debe configurarse esta dirección como dirección de interfaz en el direccionador que realiza la función de servidor TN3270.

Cuando el servidor TN3270 esté en el mismo direccionador que Network Dispatcher, se aplica lo siguiente:

- La dirección IP de servidor TN3270 para el servidor TN3270 interno debe definirse en la dirección de cluster, pero para el servidor interno, esta dirección no debe definirse en el direccionador como dirección IP interna o como dirección de interfaz.
- Cuando el servidor TN3270 es externo, la dirección IP de servidor TN3270 debe definirse en el direccionador como dirección IP interna o como dirección de interfaz. Cuando el servidor TN3270 es interno, la dirección IP de servidor TN3270 no debe definirse en el direccionador como dirección IP interna ni como dirección de interfaz. Un servidor TN3270 puede configurarse como interno o externo, pero no puede ser ambas cosas y no puede conmutar de un

tipo a otro. Como resultado de esto, al implementar la solución de alta disponibilidad de Network Dispatcher con servidores TN3270 internos en ambos direccionadores de Network Dispatcher, el Network Dispatcher de un direccionador no puede realizar el equilibrio de carga en el servidor TN3270 del otro direccionador. Puede realizar el equilibrio de carga de su propio servidor interno y de los servidores configurados como servidores externos.

LU explícitas y Network Dispatcher

Se debe tener un cuidado especial con la definición de LU explícita en un entorno de Network Dispatcher. Una petición de sesión para una LU implícita o explícita puede enviarse a cualquier servidor. Esto quiere decir que se tiene que definir la LU explícita en cada servidor, dado que no se conoce de antemano a qué servidor se enviará la sesión.

Utilización de Network Dispatcher con la Antememoria del servidor de la web

Debe utilizar Network Dispatcher para definir un cluster y un puerto para la Web Server Cache. Cuando defina un puerto con una modalidad de *antememoria*, se le solicitará que configure la partición de antememoria. Consulte el mandato **add port** en “Configuración y supervisión de la Antememoria del servidor de la web” en la página 207 para ver un ejemplo de ello. Es posible alterar posteriormente los valores de configuración de partición de antememoria utilizando el mandato **f webc** en el indicador `Config>` para ir directamente a la configuración de la característica de Antememoria del servidor de la web. Consulte “Utilización de la Antememoria del servidor de la web” en la página 169 y “Configuración y supervisión de la Antememoria del servidor de la web” en la página 207 para obtener más información acerca de la Función de colocación en antememoria del servidor de la web.

Utilización de Network Dispatcher con la Antememoria de eNetwork Host On-Demand Client

Debe utilizar Network Dispatcher para definir un cluster y un puerto para la Antememoria de Host On-Demand Client. Cuando defina un puerto con una modalidad de *antememoria de HOD client*, se le solicitará que configure la partición de antememoria. Consulte el mandato **add port** en “Configuración de la Antememoria de Host On-Demand Client” en la página 155 para ver un ejemplo de ello. Es posible alterar posteriormente los valores de configuración de partición de antememoria utilizando el mandato **f hod** en el indicador `Config>` para ir directamente a la configuración de la característica de Antememoria de Host On-Demand Client. Consulte “Configuración y supervisión de la Antememoria de IBM eNetwork Host On-Demand Client” en la página 155 para obtener más información acerca de la Antememoria de Host On-Demand Client.

Utilización de Network Dispatcher con la Antememoria escalable de alta disponibilidad (SHAC)

Esta sección describe la utilización de Network Dispatcher con la Antememoria escalable de alta disponibilidad (SHAC); la Figura 9 en la página 123 muestra un diagrama de una SHAC en una red. La Antememoria escalable de alta disponibilidad (SHAC) consiste en un grupo de antememorias de Web Server más un

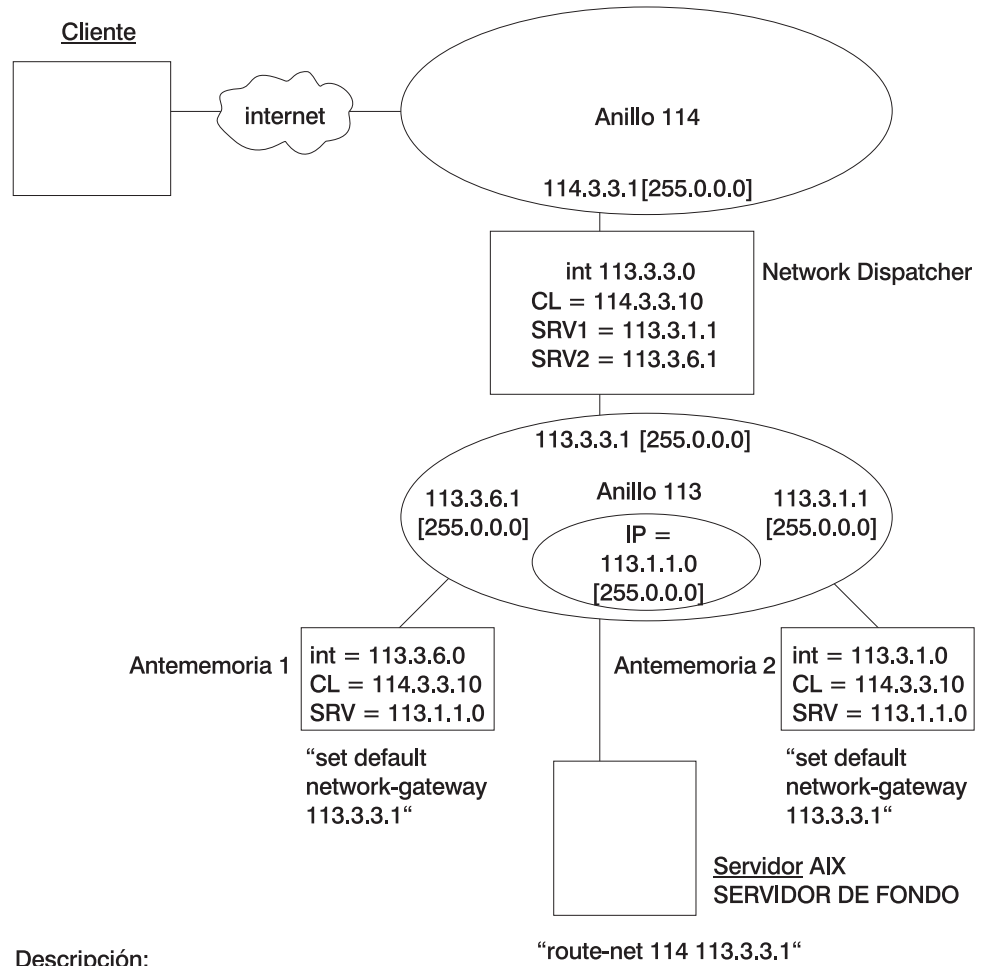
Utilización de Network Dispatcher

Network Dispatcher independiente; las antememorias están configuradas como servidores en el Network Dispatcher. Las antememorias de un grupo comparten un cluster y un puerto comunes. En Network Dispatcher se programan los valores idénticos de cluster y puerto. La modalidad del puerto se define como extcache para indicar que alimenta una matriz de antememoria escalable externa. Consulte el mandato **add port** en “Add” en la página 126.

Nota: Puede haber más de un grupo de antememorias ubicado en el Network Dispatcher.

El consejero y el gestor son de importancia crítica para SHAC. Es preciso habilitar el consejero HTTP en cualquier puerto para la que haya unas SHAC. Las consultas del consejero se utilizan para determinar si las antememorias configuradas son operativas. Inicialmente, al establecerse las conexiones, éstas se direccionan a antememorias basadas en el gestor. Por consiguiente, las proporciones del gestor se deben definir de tal manera que incorporen el consejero. Esto es importante si las antememorias se habilitan o inhabilitan.

Como otros servidores, las direcciones IP de interfaz de las antememorias se utilizan para las direcciones de servidor. La Figura 9 en la página 123 muestra un ejemplo de ello. Incluye las direcciones IP, las máscaras de red y la información de direccionamiento más importantes. En la práctica, la mayoría de los clientes están ubicados en Internet. En cualquier caso, la ruta desde el cliente a las antememorias debe pasar por el Network Dispatcher (por consiguiente, no se puede conectar a los clientes al anillo 113 de la imagen).



Descripción:

CL: Dirección de cluster. Nota - este ejemplo supone que se utiliza el puerto 80, el puerto http por omisión.

INT: Dirección interna para el direccionador 22XX

SRV: Dirección(es) de servidor asociada(s) con CL

"...": Mandatos de direccionamiento adicionales para establecer la conectividad.

Figura 9. Dos antememorias con Network Dispatcher, cliente y servidor de fondo

Configuración y supervisión de la característica Network Dispatcher

Este capítulo describe la configuración y los mandatos operativos de la característica Network Dispatcher. Contiene las secciones siguientes:

- “Acceso a los mandatos de configuración de Network Dispatcher”
- “Mandatos de configuración de Network Dispatcher”
- “Acceso a los mandatos de supervisión de Network Dispatcher” en la página 145
- “Mandatos de supervisión de Network Dispatcher” en la página 145

Acceso a los mandatos de configuración de Network Dispatcher

Para acceder al entorno de configuración de Network Dispatcher:

1. Entre **talk 6** en el indicador OPCON (*).
2. Entre **feature ndr** en el indicador Config >.

Mandatos de configuración de Network Dispatcher

La Tabla 13 contiene un resumen de los mandatos de configuración de Network Dispatcher y en el resto de esta sección se explican estos mandatos. Entre estos mandatos en el indicador NDR Config >.

Tabla 13. Mandatos de configuración de Network Dispatcher

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxiv.
Add	Configura diversos componentes de Network Dispatcher, incluidos los consejeros, clusters, puertos y servidores.
Clear	Borra toda la configuración de Network Dispatcher.
Disable	Inhabilita los componentes de copia de seguridad, ejecutor y gestor de Network Dispatcher. También inhabilita consejeros específicos.
Enable	Habilita los componentes de copia de seguridad, ejecutor y gestor de Network Dispatcher. También habilita consejeros específicos.
List	Visualiza toda la configuración de Network Dispatcher o partes específicas de la misma.
Remove	Elimina partes específicas de la configuración de Network Dispatcher.
Set	Cambia los parámetros de configuración para los consejeros, clusters, puertos, servidores o el gestor de Network Dispatcher.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiv.

Add

Utilice el mandato **add** para configurar consejeros, clusters, puertos, servidores y direcciones de alcance. Para la Alta disponibilidad, también puede configurar si este Network Dispatcher es primario o de copia de seguridad y qué direcciones IP deben utilizarse para el heartbeat y la sincronización de bases de datos.

Sintaxis:

```

add          advisor . . .
               backup . . .
               cluster . . .
               hearbeat . . .
               port . . .
               reach . . .
               server . . .
    
```

Advisor *name port# interval timeout comm-port*

Especifica el nombre y el puerto de un consejero. Este parámetro especifica también con cuánta frecuencia el consejero reunirá información sobre un protocolo específico y un período de tiempo después del cual el consejero considera que el protocolo deja de estar disponible.

name Especifica el tipo de consejero.

Tabla 14. Nombres de consejero y números de puerto

Número de consejero	Nombre de consejero	Puerto por omisión
0	FTP	21
1	HTTP	80
2	MVS	10007
3	TN3270	23
4	SMTP	25
5	NNTP	119
6	POPS	110
7	TELNET	23

Valores válidos: 0 - 7

Valor por omisión: 1

port# Especifica el número de puerto para este consejero.

Valores válidos: 1 a 65535

Valores por omisión: consulte la Tabla 14.

interval Especifica la frecuencia, en segundos, con que el consejero consulta su protocolo para cada servidor. Después de pasada la mitad de este valor sin obtener una respuesta del servidor, el consejero considera que el protocolo no está disponible.

Valores válidos: 0 a 65535

Valor por omisión: 5

timeout Especifica el intervalo de tiempo, en segundos, tras el cual el consejero considera que el protocolo no está disponible.

Para asegurarse de que el gestor no utiliza información desfasada en sus decisiones sobre equilibrio de carga, el gestor no utilizará la información del consejero cuya indicación de la hora sea más antigua que la hora definida en este parámetro. Para el consejero, el tiempo de espera debe ser mayor que el intervalo de sondeo. Si el tiempo de espera es menor, el gestor pasará por alto los informes que se deben utilizar. Por omisión, los informes del consejero no exceden un determinado tiempo de espera.

Normalmente, este valor de tiempo de espera se aplica si se inhabilita un consejero. No confunda este parámetro con el tiempo de espera intervalo/2 descrito anteriormente, que está relacionado con un servidor que no responde.

Valores válidos: 0 a 65535

Valor por omisión: 0, lo que quiere decir que se considera que el protocolo está disponible siempre.

Comm-port

Especifica el número de puerto utilizado por el consejero TN3270 para comunicar con los servidores TN3270. Este parámetro es de sólo entrada para el consejero TN3270.

Valores válidos: 1 a 65535

Valor por omisión: 10008

Nota: Dado que el componente gestor es un prerrequisito para el consejero, debe habilitar el gestor antes de que pueda habilitarse cualquier consejero. También debe definir las proporciones del gestor, de manera que el gestor tenga en cuenta la entrada del consejero al definir los pesos de servidor que se utilizan para tomar las decisiones sobre equilibrio de carga. También debe definir la dirección IP interna utilizando el mandato **set internal-ip-address** para que el consejero se ejecute correctamente. Consulte el capítulo Configuring and Monitoring IP del manual *Consulta de configuración y supervisión de protocolos Volumen 1* para obtener más información acerca del mandato **set internal-ip-address**.

Ejemplo 1:

```
add advisor
Advisor name (0=ftp,1=http,2=MVS,3=TN3270,4=smtplib,5=nntp,6=pop3,7=telnet) [1]? 1
Port number [80]?
Interval (seconds) [5]? 10
Timeout (0=unlimited) [0]? 10
```

Ejemplo 2:

```
add advisor
Advisor name (0=ftp,1=http,2=MVS,3=TN3270,4=smtplib,5=nntp,6=pop3,7=telnet) [1]? 3
Port number [23]?
Interval (seconds) [5]? 10
Timeout (0=unlimited) [0]? 10
Communication Port number [10008]?
```

Configuración de Network Dispatcher

backup *role strategy*

Especifica si este Network Dispatcher es primario o una copia de seguridad.

role Define si es un Network Dispatcher primario o de copia de seguridad. Utilice este mandato sólo si tiene la intención de tener una configuración redundante y quiere que se ejecute la función de Alta disponibilidad. En este caso debe configurar también el Heartbeat (**add heartbeat**) y la capacidad de alcance (**add reach**).

Valores válidos: 0 ó 1

0 = primario

1 = copia de seguridad

Valor por omisión: 0

strategy Especifica si Network Dispatcher conmutará a la modalidad primaria de forma automática o manual. Siempre que un Network Dispatcher primario tenga una anomalía y pase a estar en modalidad de espera (lo que quiere decir que una copia de seguridad ha ejecutado la función de entrada en función de IP) y después quede disponible, se convertirá automáticamente en el Network Dispatcher activo si la estrategia está definida como *automática*, tan pronto como se hayan sincronizado las bases de datos. Si la estrategia está definida como *manual*, el antiguo primario pasará a la modalidad de espera y el operador deberá utilizar el mandato **switchover** de talk 5 para volver a activarlo. Vea “Switchover” en la página 152.

Valores válidos: 0 ó 1

0 = automático

1 = manual

Valor por omisión: 0

Ejemplo:

```
add backup
Role (0=Primary, 1=Backup) [0]?
Switch back strategy (0=Auto, 1=Manual) [0]?
```

cluster *address FIN-count FIN-timeout Stale-timer*

Especifica una dirección IP del cluster y la frecuencia con la que el ejecutor realiza la recogida de basura de la base de datos de Network Dispatcher. Network Dispatcher no anuncia específicamente las direcciones de cluster, de manera que deben seleccionarse las direcciones de cluster que formen parte de una subred anunciada que sea local respecto al direccionador de Network Dispatcher. Habitualmente, esto sería la subred en la que Network Dispatcher recibe el tráfico de cliente desde el siguiente direccionador de salto.

Nota: Las Direcciones IP de cluster no deben coincidir con la dirección IP interna del direccionador y no debe coincidir con ninguna dirección IP de interfaz definida en el direccionador.

address Especifica la dirección IP del cluster.

Valores válidos: cualquier dirección IP válida

Valor por omisión: 0.0.0.0

FIN-count

Especifica el número de conexiones que deben estar en estado FIN antes de que el ejecutor intente eliminar la información de conexión no utilizada de la base de datos de Network Dispatcher, después de que haya transcurrido el tiempo indicado en *FIN-timeout* o *Stale-timer*.

Valores válidos: de 0 a 65535

Valor por omisión: 4000

FIN-timeout

Especifica el número de segundos que una conexión ha permanecido en el estado FIN, después de lo cual el ejecutor intenta eliminar la información de conexión no utilizada de la base de datos de Network Dispatcher.

Valores válidos: de 0 a 65535

Valor por omisión: 30

Stale-timer

Especifica el número de segundos que una conexión ha permanecido inactiva, después de lo cual el ejecutor intenta eliminar la información de la conexión de la base de datos de Network Dispatcher.

Valores válidos: de 0 a 65535

Valor por omisión: 1500

Ejemplo:

```
NDR Config>add cluster
Cluster Address [0.0.0.0]? 113.3.1.12
FIN count [4000]?
FIN time out [30]?
Stale timer [1500]?
Cluster 113.3.1.12 has been added.
Fincount has been set to 4000 for cluster 113.3.1.12
Fintimeout has been set to 30 for cluster 113.3.1.12
Staletimer has been set to 1500 for cluster 113.3.1.12
NDR Config>
```

heartbeat *address1 address2*

Especifica una vía de acceso para los mensajes Heartbeat. Es recomendable que configure más de una entrada para conseguir un funcionamiento fiable. El mensaje Heartbeat circulará desde *address1*, que pertenece a este Network Dispatcher, a *address2*, que pertenece al Network Dispatcher similar.

address1 Especifica la dirección IP de la interfaz de este Network Dispatcher desde el que circularán los mensajes Heartbeat.

Valores válidos: cualquier dirección IP.

Valor por omisión: 0.0.0.0

address2 Especifica la dirección IP de la interfaz del Network Dispatcher similar hacia el que circularán los mensajes Heartbeat. Esta dirección se debe poder alcanzar desde la interfaz especificada en *address1*.

Valores válidos: cualquier dirección IP.

Valor por omisión: 0.0.0.0

Ejemplo:

```
add heartbeat
Source Heartbeat address [0.0.0.0]? 131.2.25.90
Target Heartbeat Address [0.0.0.0]? 131.2.25.92
```

port cluster-address port# port-type max-weight port-mode

Especifica el puerto y sus atributos.

cluster-address

Especifica la dirección IP del cluster.

Valores válidos: cualquier dirección IP.

Valor por omisión: 0.0.0.0

port# Especifica el número de puerto del protocolo para este cluster.

Valores válidos: 1 a 65535

Valor por omisión: 80

port-type Especifica los tipos de tráfico IP en los que se puede establecer el equilibrio de carga en este puerto. Los tipos soportados son:

- 1 = TCP
- 2 = UDP
- 3 = ambos

Valores válidos: 1, 2, 3

Valor por omisión: 3

max-weight

Especifica el peso máximo de los servidores en este puerto. Esto afecta al grado de diferencia que puede existir entre el número de peticiones que el ejecutor proporcionará a cada servidor.

Valores válidos: 0 a 100

Valor por omisión: 20

port-mode

Especifica si el puerto proveerá todas las peticiones de un único cliente a un único servidor (conocido como "sticky"), utilizará el ftp pasivo (pftp), utilizará la Antememoria del servidor de la web (cache), proveerá una matriz de antememoria escalable externa (extcache), utilizará la Antememoria de Host On-Demand Client, o no utilizará ningún protocolo en particular en este cluster (none).

Valores válidos: 0 - 5, donde:

- 0 = none
- 1 = sticky
- 2 = pftp
- 3 = cache
- 4 = extcache
- 5 = hod client cache

Valor por omisión: 0

Ejemplo:

```
Config>feature ndr
NDR>add cluster 1.2.3.4 4000 30 1500
NDR>add port
Cluster address [0.0.0.0]? 1.2.3.4
Port number [80]? 80
Port type [3]?
Maximum weight [20]?
Port mode [0=none, 1=sticky, 2=pftp, 3=cache 4=extcache 5=hod client cache ]? 0
```

Notas:

1. Cuando se seleccione la modalidad de puerto 3 (cache=3), consulte “Configuración y supervisión de la Antememoria del servidor de la web” en la página 207 para obtener información acerca de la Antememoria del servidor de la web.
2. Cuando se seleccione la modalidad de puerto 5 (hod client cache=5), consulte “Configuración y supervisión de la Antememoria de IBM eNetwork Host On-Demand Client” en la página 155 para obtener información acerca de la Antememoria del servidor de la web.

reach address

Especifica cualquier dirección de sistema principal que Network Dispatcher debe poder alcanzar para ejecutarse correctamente. Puede ser una dirección de servidor, una dirección de direccionador, una dirección de estación de administración u otro sistema principal IP.

address Especifica la dirección IP de destino.

Valores válidos: cualquier dirección IP

Valor por omisión: 0.0.0.0

Ejemplo:

```
add reach
Address to reach [0.0.0.0]?
```

server cluster-address port# server-address server-weight server-state

Especifica los atributos de un servidor en un cluster.

cluster-address

Especifica la dirección IP del cluster al que pertenece este servidor.

Valores válidos: cualquier dirección IP

Valor por omisión: 0.0.0.0

Configuración de Network Dispatcher

port# Especifica el protocolo que se ejecuta en este servidor a través de la conexión.

Valores válidos: 1 a 65535

Valor por omisión: 80

server-address

Especifica la dirección IP del servidor.

Valores válidos: cualquier dirección IP

Valor por omisión: 0.0.0.0

server-weight

Especifica el peso del servidor para el ejecutor. Esto afecta a la frecuencia con que Network Dispatcher envía peticiones a este servidor específico.

Valores válidos: de 0 al valor de *max-weight* que se ha especificado en el mandato add port.

Valor por omisión: max-weight en el mandato port

server-state

Especifica si el ejecutor debe considerar que el servidor está disponible o no cuando el ejecutor empieza a procesar.

Valores válidos: 0 (desactivado) ó 1 (activado)

Valor por omisión: 1

Ejemplo:

```
add server
Cluster address [0.0.0.0]? 131.2.25.91
Port number [80]? 80
Server address [0.0.0.0]? 131.2.25.94
Server weight [35]?
Server state (down=0 up=1) [1]?
```

Límites de configuración de los parámetros

La Tabla 15 lista los límites para los diversos elementos que puede configurar para un Network Dispatcher.

Parámetro	Límite
Advisors	32 por 2216
Clusters	100 por 2216
Heartbeats	32 por 2216
Ports	32 por cluster
Reachs	32 por 2216
Servers	128 por cada puerto configurado, 512 para cada número de puerto bajo todos los clusters configurados para 2216.
Dirección IP exclusiva de servidor	128 por 2216

Clear

Utilice el mandato **clear** para borrar la configuración completa de Network Dispatcher.

Sintaxis:

clear

Disable

Utilice el mandato **disable** para inhabilitar un componente de Network Dispatcher.

Sintaxis:

disable advisor . . .
 backup
 executor
 manager

advisor *name port#*

Inhabilita un consejero de Network Dispatcher.

name Especifica el tipo de consejero.

Consulte la Tabla 14 en la página 126 para obtener información adicional.

Valores válidos: 0 - 7

Valor por omisión: 0

port# Especifica el número de puerto para este consejero.

Valores válidos: 1 a 65535

Valor por omisión: ninguno. Debe entrar un número de puerto.

Ejemplo:

```
disable advisor
Advisor name (0=ftp,1=http,2=MVS,3=TN3270,4=smt,5=nntp,6=pop3,7=telnet) [1]? 1
Port number [0]? 80
```

backup Inhabilita la función de copia de seguridad de Network Dispatcher.

Ejemplo:

```
disable backup
Backup is now disabled.
```

executor Inhabilita el ejecutor de Network Dispatcher. La inhabilitación del ejecutor inhabilita la característica Network Dispatcher.

Ejemplo:

```
disable executor
Executor is now disabled.
```

Nota: La inhabilitación del ejecutor detendrá el gestor, consejeros y la función de alta disponibilidad, si se están ejecutando actualmente.

Configuración de Network Dispatcher

manager Inhabilita el gestor de Network Dispatcher. El gestor es un componente opcional. No obstante, si no utiliza el gestor, Network Dispatcher realizará el equilibrio de carga mediante un método de planificación rotatorio, basado en los pesos de servidor actuales.

Ejemplo:

```
disable manager
Manager is now disabled.
```

Nota: Dado que el componente gestor es un prerrequisito para los consejeros, la inhabilitación del gestor detendrá la ejecución de todos los consejeros.

Enable

Utilice el mandato **enable** para habilitar un componente de Network Dispatcher.

Sintaxis:

```
enable          advisor . . .
                  backup
                  executor
                  manager
```

advisor name port#

Habilita un consejero en Network Dispatcher.

name Especifica el tipo de consejero.

Consulte la Tabla 14 en la página 126 para obtener información adicional.

Valores válidos: 0 - 7

Valor por omisión: 0

port# Especifica el número de puerto para este consejero.

Valores válidos: 1 a 65535

Valor por omisión: ninguno. Debe entrar un número de puerto.

Ejemplo:

```
enable advisor
Advisor name (0=ftp,1=http,2=MVS,3=TN3270,4=smtp,5=nntp=6=pop3,7=telnet) [1]? 1
Port number [0]? 80
```

Nota: Dado que el componente gestor es un prerrequisito para el consejero, debe habilitar el gestor antes de que pueda habilitarse cualquier consejero. También debe definir las proporciones del gestor, de manera que el gestor tenga en cuenta la entrada del consejero al definir los pesos de servidor que se utilizan para tomar las decisiones sobre equilibrio de carga. También debe definir la dirección IP interna utilizando el mandato **set internal-ip-address** para que el consejero se ejecute correctamente. Consulte el capítulo Configuring and Monitoring IP en *Consulta de configuración y supervisión de protocolos Volumen 1* para obtener más información acerca del mandato **set internal-ip-address**.

backup Habilita la función de copia de seguridad de Network Dispatcher.

Ejemplo: enable backup

Nota: Antes de habilitar la copia de seguridad, debe añadir un heartbeat por lo menos.

executor Habilita el ejecutor de Network Dispatcher.

Ejemplo:

```
enable executor
Executor is now enabled.
```

manager Habilita el gestor de Network Dispatcher.

Ejemplo:

```
enable manager
Manager interval was set to 2.
Manager proportions were set to 50 50 0 0
Manager refresh cycle was set to 2
Manager sensitivity was set to 5.
Manager smoothing factor was set to 1.50.
```

Cuando el gestor se habilita por primera vez, se crea un registro del gestor con los siguientes valores por omisión:

Intervalo: 2 segundos

Ciclo de renovación: 2

Sensibilidad: 5 %

Alisado: 1,5

Proporciones:

Activa: 50%

Nueva: 50%

Consejero: 0

Sistema: 0

Consulte "Set" en la página 139 para ver una descripción de los parámetros antedichos.

List

Utilice el mandato **list** para visualizar información acerca de Network Dispatcher.

Sintaxis:

```
list          all
              advisor
              backup
              cluster
              manager
              port
              server
```

Configuración de Network Dispatcher

all Visualiza toda la información de configuración de Network Dispatcher. Incluye la misma información que se visualiza para los consejeros, la copia de seguridad, el cluster, el gestor, los puertos y los servidores.

Ejemplo:

```
NDR Config> list all
```

```
Executor: Enabled
```

```
Manager: Enabled
```

```
Interval      Refresh-Cycle  Sensitivity    Smoothing
2             2              5 %           1.50
Proportions:  Active New      Advisor       System
50 %  50 %    0 %          0 %
```

```
Advisor:
```

```
Name  Port  Interval  TimeOut  State  CommPort
http  80    5         0        Enabled
MVS   10007 15        0        Enabled
TN3270 23    5         0        Enabled 10008
```

```
Backup: Enabled
```

```
Role      Strategy
PRIMARY   AUTOMATIC
```

```
Reachability: Address      Mask          Type
131.2.25.93  255.255.255.255 HOST
131.2.25.94  255.255.255.255 HOST
```

```
HeartBeat Configuration:
```

```
Source Address: 131.2.25.90 Target Address: 131.2.25.92
Source Address: 132.2.25.90 Target Address: 132.2.25.92
```

```
Clusters:
```

```
Cluster-Addr  FIN-count  FIN-timeout  Stale-timer
131.2.25.91   4000       30           1500
```

```
Ports:
```

```
Cluster-Addr  Port#  Weight  Port-Mode  Port-Type
131.2.25.91   23    20 %   none      TCP
131.2.25.91   80    20 %   none      Both
```

```
Servers:
```

```
Cluster-Addr  Port#  Server-Addr  Weight  State
131.2.25.91   23    131.2.25.93  20 %   up
131.2.25.91   23    131.2.25.94  20 %   up
131.2.25.91   80    131.2.25.93  20 %   up
131.2.25.91   80    131.2.25.94  20 %   up
```

advisor Visualiza la configuración de los consejeros de Network Dispatcher.

backup Visualiza la configuración de la copia de seguridad de Network Dispatcher.

cluster Visualiza la configuración de los clusters de Network Dispatcher.

manager Visualiza la configuración del gestor de Network Dispatcher.

port Visualiza la configuración de los puertos de Network Dispatcher.

server Visualiza la configuración de los servidores asociados a los clusters de Network Dispatcher.

Remove

Utilice el mandato **remove** para suprimir parte de la configuración de Network Dispatcher.

Sintaxis:

```
remove      advisor . . .
```

```
backup
```

cluster . . .
heartbeat . . .
port . . .
reach . . .
server . . .

advisor *name port#*

Elimina un consejero específico de la configuración de Network Dispatcher.

name Especifica el tipo de consejero.
 Consulte la Tabla 14 en la página 126 para obtener información adicional.

Valores válidos: 0 - 7

Valor por omisión: 0

port# Especifica el número de puerto para este consejero.

Valores válidos: 1 a 65535

Valor por omisión: ninguno. Debe entrar un número de puerto.

Ejemplo:

```
remove advisor
Advisor name (0=ftp,1=http,2=MVS,3=TN3270,4=smt,5=nntp,6=pop3,7=telnet) [0]?
Advisor port [0]? 80
```

backup Elimina la función de alta disponibilidad.

Nota: Dado que la copia de seguridad es un prerequisite para las funciones heartbeat y reach, la eliminación de la copia de seguridad detendrá la ejecución de heartbeat y reach.

Ejemplo: remove backup

cluster *address*

Elimina un cluster de la configuración de Network Dispatcher.

address Especifica la dirección IP del cluster.

Valores válidos: cualquier dirección IP válida

Valor por omisión: 0.0.0.0

Nota: La eliminación de una dirección de cluster causa también la eliminación de todos los puertos y los servidores asociados a ese cluster.

Ejemplo:

```
remove cluster
WARNING: Deleting a cluster will make any port or server
associated with it to also be deleted.
Cluster address [0.0.0.0]? 131.2.25.91
```

heartbeat *address*

Elimina la dirección de heartbeat de la configuración de Network Dispatcher.

Configuración de Network Dispatcher

address Especifica la dirección IP para el Network Dispatcher de destino.

Valores válidos: cualquier dirección IP válida

Valor por omisión: 0.0.0.0

Ejemplo:

```
remove heartbeat
Target address [0.0.0.0]? 131.2.25.92
```

port *cluster-address port#*

Elimina un puerto de un cluster específico de la configuración de Network Dispatcher.

cluster-address

Especifica la dirección IP del cluster.

Valores válidos: cualquier dirección IP.

Valor por omisión: 0.0.0.0

port# Especifica el número de puerto del protocolo para este cluster.

Valores válidos: 1 a 65535

Valor por omisión: ninguno. Debe entrar un número de puerto.

Notas:

1. La eliminación de un puerto causará también la eliminación de todos los servidores asociados a ese puerto.
2. Si la modalidad de puerto para el puerto que se elimina es antememoria, también se eliminará la configuración del Proxy de Antememoria del servidor de la web asociado.
3. Si la modalidad de puerto para el puerto que se elimina es Host On-Demand Client Cache, también se eliminará la configuración del Proxy de Antememoria de Host On-Demand Client asociado.

Ejemplo:

```
remove port
WARNING: Deleting a port will make any server
associated with it also be deleted. [0.0.0.0]? 7.82.142.15
Port number [0]? 80
Cluster address [0.0.0.0]? 20.21.22.15
```

reach *address*

Elimina un servidor de la lista de sistemas principales que Network Dispatcher debe poder alcanzar.

address Especifica la dirección IP del cluster.

Valores válidos: cualquier dirección IP.

Valor por omisión: 0.0.0.0

Ejemplo:

```
remove reach
Target address [0.0.0.0]? 9.82.142.15
```

server *cluster-address port# server-address*

Elimina un servidor de un cluster y de un puerto de la configuración de Network Dispatcher.

cluster-address

Especifica la dirección IP del cluster.

Valores válidos: cualquier dirección IP.

Valor por omisión: 0.0.0.0

port#

Especifica el número de puerto del protocolo para este cluster.

Valores válidos: 1 a 65535

Valor por omisión: ninguno. Debe entrar un número de puerto.

server-address

Especifica la dirección IP del cluster.

Valores válidos: cualquier dirección IP.

Valor por omisión: 0.0.0.0

Ejemplo:

```
remove server
Cluster address [0.0.0.0]? 7.82.142.15
Port number [0]? 80
Server address [0.0.0.0]? 20.21.22.15
```

Set

Utilice el mandato **set** para cambiar los atributos de un consejero, cluster, puerto o servidor existente. También puede definir atributos para el gestor de Network Dispatcher.

Sintaxis:

```
set          advisor . . .
              cluster . . .
              manager . . .
              port . . .
              server . . .
```

advisor *name port# interval timeout comm-port*

Cambia el número de puerto, el intervalo y el tiempo de espera de un consejero.

name Especifica el tipo de consejero.

Consulte la Tabla 14 en la página 126 para obtener información adicional.

Valores válidos: 0 - 7

Valor por omisión: 0

port#

Especifica el número de puerto para este consejero.

Valores válidos: 1 a 65535

Valor por omisión: ninguno. Debe entrar un número de puerto.

interval Especifica la frecuencia con que el consejero consulta su protocolo para cada servidor. Después de que haya caducado la mitad de este valor sin obtener una respuesta del servidor, el consejero considera que el protocolo no está disponible.

Valores válidos: 0 a 65535

Valor por omisión: 5

timeout Especifica el intervalo de tiempo, en segundos, tras el cual el consejero considera que el protocolo no está disponible.

Para asegurarse de que el gestor no utiliza información desfasada en sus decisiones sobre equilibrio de carga, el gestor no utilizará la información del consejero cuya indicación de la hora sea más antigua que la hora definida en este parámetro. Para el consejero, el tiempo de espera debe ser mayor que el intervalo de sondeo. Si el tiempo de espera es menor, el gestor pasará por alto los informes que se deben utilizar. Por omisión, los informes del consejero no exceden un determinado tiempo de espera.

Normalmente, este valor de tiempo de espera se aplica si se inhabilita un consejero. No confunda este parámetro con el tiempo de espera $\text{interval}/2$ descrito anteriormente, que está relacionado con un servidor que no responde.

Valores válidos: 0 a 65535

Valor por omisión: 0, lo que quiere decir que se considera que el protocolo está disponible siempre.

comm-port

Especifica el número de puerto utilizado por el consejero TN3270 para comunicar con los servidores TN3270. Este parámetro es de sólo entrada para el consejero TN3270.

Valores válidos: 1 a 65535

Valor por omisión: 10008

Ejemplo:

```
set advisor
Advisor name (0=ftp,1=http,2=MVS,3=TN3270,4=smtsp,5=nntp=6=pop3,7=telnet) [0]?
Port number [0]? 21
Interval (seconds) [5]? 10
Timeout (0=unlimited) [0]? 20
```

cluster address FIN-count FIN-timeout Stale-timer

Cambia los valores de FIN-count, FIN-timeout y Stale-timer para un cluster en la configuración de Network Dispatcher.

address Especifica la dirección IP del cluster.

Valores válidos: cualquier dirección IP válida

Valor por omisión: 0.0.0.0

FIN-count

Especifica el número de conexiones que deben estar en estado FIN antes de que el ejecutor intente eliminar la información de conexión no utilizada de la base de datos de

Network Dispatcher, después de que haya transcurrido el tiempo indicado en *FIN-timeout* o *Stale-timer*.

Valores válidos: de 0 a 65535

Valor por omisión: 4000

FIN-timeout

Especifica el número de segundos después de los cuales el ejecutor intentará eliminar la información de conexión no utilizada de la base de datos de Network Dispatcher.

Valores válidos: de 0 a 65535

Valor por omisión: 30

Stale-timer

Especifica el número de segundos que una conexión ha permanecido inactiva, después de los cuales el ejecutor intentará eliminar la información de una conexión de la base de datos de Network Dispatcher.

Valores válidos: de 0 a 65535

Valor por omisión: 1500

Ejemplo:

```
set cluster
Cluster address [0.0.0.0]? 131.2.25.91
FIN count [4000]? 4500
FIN timeout [30]? 40
Stale timer [1500]? 2000
```

manager *interval proportion refresh sensitivity smoothing*

Define los valores que utiliza el gestor para determinar cuál es el mejor servidor para satisfacer una petición.

interval Especifica el tiempo, en segundos, tras el cual el gestor actualiza los pesos de los servidores que utiliza el ejecutor en las conexiones de equilibrio de carga.

Valores válidos: 0 a 65535

Valor por omisión: 2

proportion

Especifica la importancia relativa de los factores externos en las decisiones del gestor sobre los pesos. La suma de las proporciones debe ser igual a 100. Los factores son:

active Número de conexiones activas en cada servidor TCP/IP, tal como el ejecutor ha realizado el seguimiento.

Valores válidos: 0 a 100

Valor por omisión: 50

new Número de conexiones nuevas en cada servidor TCP/IP, tal como el ejecutor ha realizado el seguimiento.

Valores válidos: 0 a 100

Valor por omisión: 50

Configuración de Network Dispatcher

advisor Entrada de los consejeros de protocolo definidos en Network Dispatcher.

Valores válidos: 0 a 100

Valor por omisión: 0

system Entrada del consejero del sistema MVS proporcionada por la herramienta de supervisión del sistema WLM MVS.

Valores válidos: 0 a 100

Valor por omisión: 0

refresh Especifica la frecuencia con que el gestor solicita el estado del ejecutor. Este parámetro se especifica como un número de *intervalos*.

Valores válidos: 0 a 100

Valor por omisión: 2

sensitivity

Especifica el cambio de pesos porcentuales para todos los servidores en un puerto, tras el cual el gestor actualizará los pesos que utiliza el ejecutor en las conexiones de equilibrio de carga.

Valores válidos: 0 a 100

Valor por omisión: 5

smoothing

Especifica un límite a la cantidad que el peso de un servidor puede modificar. El alisado minimiza la frecuencia de cambio en la distribución de las peticiones. Un índice de alisado más elevado hará que los pesos cambien menos. En cambio, un índice de alisado más pequeño hará que los pesos cambien más.

Valores válidos: un valor decimal entre 1,0 y 42 949 673,00

Valor por omisión: 1,5

Nota: Sólo puede especificar dos posiciones después de la coma decimal.

Ejemplo:

```
set manager
Interval (in seconds) [2]? 3
Active proportion [50]? 40
New proportion [50]? 38
Advisor proportion [0]? 20
System proportion [0]? 2
Refresh cycle [2]? 4
Sensitivity threshold [5]? 10
Smoothing index (>1.00) [1.50]? 200
```

port cluster-address port# port-type max-weight port-mode

Cambia el tipo de puerto, el peso máximo y la modalidad de puerto para un cluster y un número de puerto específicos.

cluster-address

Especifica la dirección IP del cluster.

Valores válidos: cualquier dirección IP.

Valor por omisión: 0.0.0.0

port# Especifica el número de puerto del protocolo para este cluster.

Valores válidos: 1 a 65535

Valor por omisión: ninguno. Debe entrar un número de puerto.

port-type Especifica el tipo de tráfico IP para el que se puede establecer el equilibrio de carga en esta puerto.

Valores válidos:

tcp=1

udp=2

ambos=3

Valor por omisión: 3

max-weight

Especifica el peso de los servidores en esta puerto. Esto afecta al grado de diferencia que puede existir entre el número de peticiones que el ejecutor proporcionará a cada servidor.

Valores válidos: 0 a 100

Valor por omisión: 20

port-mode

Especifica si el puerto proveerá todas las peticiones de un único cliente a un único servidor (conocido como "sticky"), utilizará el ftp pasivo (pftp), utilizará la Antememoria del servidor de la web (cache), proveerá una matriz de antememoria escalable externa, utilizará la Antememoria de Host On-Demand Client, o no utilizará ningún protocolo en este cluster (none).

Valores válidos:

none=0

sticky=1

pftp=2

cache=3

extcache=4

hod client cache=5

Valor por omisión: 0 (none)

Ejemplo:

```
set port
Cluster address [0.0.0.0]? 131.2.25.91
Port number [0]? 23
Port type (tcp=1, udp=2, both=3) [3]?
Max. weight (0-100) [20]? 30
Port mode (none=0, sticky=1, pftp=2, cache=3, extcache=4 hod client cache=5) [0]?
```

Notas:

1. Cuando se seleccione la modalidad de puerto 3 (cache=3), consulte “Configuración y supervisión de la Antememoria del servidor de la web” en la página 207 para obtener información acerca de la Antememoria de Web Server.
2. Cuando se seleccione la modalidad de puerto 5 (hod client cache=5), consulte “Configuración y supervisión de la Antememoria de IBM eNetwork Host On-Demand Client” en la página 155 para obtener información acerca de la Antememoria de Web Server.

server *cluster-address port# server-address weight state*

Cambia el estado y el peso de servidor para un servidor específico de un cluster.

cluster-address

Especifica la dirección IP del cluster al que pertenece este servidor.

Valores válidos: cualquier dirección IP

Valor por omisión: 0.0.0.0

port# Especifica el número de puerto del protocolo para este cluster.

Valores válidos: 1 a 65535

Valor por omisión: ninguno. Debe entrar un número de puerto.

server-address

Especifica la dirección IP del servidor.

Valores válidos: cualquier dirección de servidor válida

Valor por omisión: 0.0.0.0

state Especifica si el ejecutor debe considerar que el servidor está disponible o no cuando el ejecutor empieza a procesar.

Valores válidos: 0 (desactivado) ó 1 (activado)

Valor por omisión: 1

weight Especifica el peso del servidor para el ejecutor. Esto afecta a la frecuencia con que Network Dispatcher envía peticiones a este servidor específico.

Valores válidos: de 0 al valor de *max-weight* que se ha especificado en el mandato add port.

Valor por omisión: max-weight en el mandato port

Ejemplo:

```
set server
Cluster address [0.0.0.0]? 131.2.25.91
Port number [0]?
Server address [0.0.0.0]?
Server weight [20]? 25
Server state (down=0, up=1) [1]? 1
```

Acceso a los mandatos de supervisión de Network Dispatcher

Para acceder al entorno de supervisión de Network Dispatcher:

1. Entre **talk 5** en el indicador OPCON (*).
2. Entre **feature ndr** en el indicador GWCON (+).

También se puede supervisar Network Dispatcher utilizando SNMP. Consulte “SNMP Management” en el manual *Consulta de configuración y supervisión de protocolos Volumen 1* para obtener más información.

Mandatos de supervisión de Network Dispatcher

La Tabla 16 contiene un resumen de los mandatos de supervisión de Network Dispatcher y en el resto de esta sección se explican estos mandatos. Entre estos mandatos en el indicador NDR >.

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxiv.
List	Visualiza los atributos configurados actualmente del consejero, los clusters, los puertos o los servidores.
Quiesce	Especifica que no se debe enviar a un servidor ninguna petición de conexión más. Además, detiene temporalmente las funciones heartbeat y reach.
Report	Visualiza un informe de información relativa al consejero y al gestor.
Status	Visualiza el estado actual de los contadores, clusters, puertos, servidores, el consejero, el gestor y la copia de seguridad.
Switchover	Obliga a un Network Dispatcher que se ejecuta en modalidad de espera a convertirse en el Network Dispatcher activo. La utilización de este mandato es necesaria si ha especificado la modalidad de conmutación manual.
Unquiesce	Permite al gestor de Network Dispatcher asignar un peso mayor que 0 a un servidor en el que se ha ejecutado quiesce previamente en cada puerto configurado por el servidor. Esta acción permite que circulen nuevas peticiones de conexión hacia el servidor seleccionado.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiv.

List

Utilice el mandato **list** para visualizar información acerca de Network Dispatcher.

Sintaxis:

```
list          _advisor
              _cluster
              port
              _server
```

Configuración de Network Dispatcher

advisor Visualiza la configuración de los consejeros de Network Dispatcher.

Ejemplo:

```
list advisor
Advisor list requested.
```

ADVISOR	PORT	TIMEOUT	STATUS
ftp	21	5	ACTIVE
Http	80	unlimited	ACTIVE
MVS	10007	unlimited	ACTIVE
TN3270	23	unlimited	ACTIVE

cluster Visualiza la configuración de los clusters de Network Dispatcher.

Ejemplo:

```
list cluster
EXECUTOR INFORMATION:
-----
Version: 01.01.00.00 - Tue Dec 10 14:15:58 EST 1996
Number of defined clusters: 2
```

```
CLUSTER LIST:
-----
131.2.25.91
10.11.12.2
```

port Visualiza la configuración de los puertos de Network Dispatcher.

Ejemplo:

```
list port
Cluster Address [0.0.0.0]? 131.2.25.91
```

PORT	MAXWEIGHT	PORT MODE	PORT TYPE
23	30	none	TCP
80	20	none	both

server Visualiza la configuración de los servidores asociados a los clusters de Network Dispatcher.

Ejemplo:

list server

Cluster Address [0.0.0.0]? **131.2.25.91**

PORT 23 INFORMATION:

```

-----
Maximum weight..... 20
Port mode..... NONE
Port type..... TCP
All up nodes are weight zero.... FALSE
Total target nodes..... 2
Currently marked down..... 0
Servers providing service to this port:
Address: 131.2.25.93 Weight: 20 Count: 0 TCP Count: 0 UPD Count: 0
Active: 0 FIN 0 Complete 0 Status: up Saved Weight: -1
Address: 131.2.25.94 Weight: 20 Count: 0 TCP Count: 0 UPD Count: 0
Active: 0 FIN 0 Complete 0 Status: up Saved Weight: -1
    
```

PORT 80 INFORMATION:

```

-----
Maximum weight..... 20
Port mode..... NONE
Port type..... BOTH
All up nodes are weight zero.... FALSE
Total target nodes..... 2
Currently marked down..... 0
Servers providing service to this port:
Address: 131.2.25.93 Weight: 20 Count: 0 TCP Count: 0 UPD Count: 0
Active: 0 FIN 0 Complete 0 Status: up Saved Weight: -1
Address: 131.2.25.94 Weight: 20 Count: 0 TCP Count: 0 UPD Count: 0
Active: 0 FIN 0 Complete 0 Status: up Saved Weight: -1
    
```

Quiesce

Utilice el mandato **quiesce** para detener temporalmente las funciones heartbeat o reach, o bien para especificar que no se debe enviar a un servidor ninguna petición de conexión más.

Sintaxis:

```

quiesce          hheartbeat
                   manager
                   reach
    
```

heartbeat *address*

Detiene la vía de acceso seleccionada para la función heartbeat. *Address* es la dirección IP del Network Dispatcher remoto al que este Network Dispatcher está enviando mensajes Heartbeat.

Ejemplo:

```

quiesce heartbeat
Remote Address [0.0.0.0]? 131.2.25.94
    
```

manager *address*

Especifica que no se debe realizar ninguna petición de conexión más al servidor especificado. *Address* es la dirección IP del servidor.

Ejemplo:

```

quiesce manager
Server Address [0.0.0.0]? 131.2.25.93
    
```

Configuración de Network Dispatcher

reach *address*

Detiene el sondeo que Network Dispatcher realiza en la dirección especificada para determinar si puede alcanzarse, donde *address* es la dirección IP que forma parte de los criterios de capacidad de alcance.

Ejemplo:

```
quiesce reach
Reach Address [0.0.0.0]? 131.2.25.92
```

Report

Utilice el mandato **report** para visualizar un informe del consejero o del gestor

Sintaxis:

```
report          advisor
                  manager
```

advisor *type port#*

Visualiza un informe de información acerca de un consejero específico.

type Es el tipo de consejero. Vea los tipos de consejero en la Tabla 14 en la página 126.

port# Es el número de puerto.

Ejemplo:

```
report advisor
0=ftp,1=http,2=MVS,3=TN3270,4=smtp,5=nntp,6=pop3,7=telnet
Advisor name [0]? 1
Port number [0]? 80
```

```
-----
|      ADVISOR:   http      |
|      PORT:     80        |
|-----|-----|
| 131.2.25.93    |         0 |
| 131.2.25.94    |         16 |
|-----|-----|
```

manager Visualiza un informe de la información actual sobre el gestor.

Ejemplo:

report manager

```
-----
| HOST TABLE LIST | STATUS |
-----
| 131.2.25.93      | ACTIVE |
| 131.2.25.94      | ACTIVE |
-----
```

```
-----
131.2.25.91 | WEIGHT | ACTIVE % 50 | NEW % 50 | PORT % 0 | SYSTEM % 0 |
-----
PORT: 23    | NOW|NEW| WT | CONNECT | WT | CONNECT | WT | LOAD | WT | LOAD |
-----
131.2.25.93 | 10| 10| 10|      0| 10|      0|  0|      0|-999| -1|
131.2.25.94 | 10| 10| 10|      0| 10|      0|  0|      0|-999| -1|
-----
PORT TOTALS: | 20| 20|      |      0|      |      0|      |      0|      | -2|
-----
```

```
-----
131.2.25.91 | WEIGHT | ACTIVE % 50 | NEW % 50 | PORT % 0 | SYSTEM % 0 |
-----
PORT: 80    | NOW|NEW| WT | CONNECT | WT | CONNECT | WT | LOAD | WT | LOAD |
-----
131.2.25.93 | 10| 10| 10|      0| 10|      1| 16|      0|-999| -1|
131.2.25.94 | 10| 10| 10|      0| 10|      1|  3|     16|-999| -1|
-----
PORT TOTALS: | 20| 20|      |      0|      |      0|     16|      | -2|
-----
```

```
-----
| ADVISOR | PORT | TIMEOUT | STATUS |
-----
| http    | 80   | unlimited | ACTIVE |
| MVS     | 10007 | unlimited | ACTIVE |
-----
```

Manager report requested.

Status

Utilice el mandato **status** para obtener el estado de los consejeros, la copia de seguridad, el contador, los clusters, el gestor, los puertos y los servidores.

Sintaxis:

- status** advisor
- backup
- cluster
- counter
- manager
- ports
- servers

advisor *name port#*

Obtiene el estado de un consejero específico.

name Especifica el tipo de consejero. Vea los tipos de consejero en la Tabla 14 en la página 126.

port# Es el número de puerto.

Configuración de Network Dispatcher

Ejemplo:

```
status advisor
0=ftp, 1=http, 2=MVS 3=TN3270, 4=SMTP, 5=NNTP, 6=POP3, 7=TELNET
Advisor name [0]?
Port number [0]? 21
```

```
Advisor ftp on port 21 status:
=====
Interval..... 10
```

backup Obtiene el estado de la función de copia de seguridad.

Ejemplo:

```
status backup
Dumping status ...
Role : PRIMARY Strategy : AUTOMATIC State : ND_ACTIVE Sub-State : ND_SYNCHRONIZED
<<Preferred Target : 132.2.25.92>>
```

```
Dumping HeartBeat Status ...
....Heartbeat target : 131.2.25.92 Status : UNREACHABLE
....Heartbeat target : 132.2.25.92 Status : REACHABLE
```

```
Dumping Reachability Status ...
....Host:131.2.25.93 Local:REACHABLE
....Host:131.2.25.94 Local:REACHABLE
```

cluster address

Obtiene el estado de un cluster específico; *address* es la dirección IP del cluster.

Ejemplo:

```
status cluster
Cluster Address [0.0.0.0]? 131.2.25.91
```

```
EXECUTOR INFORMATION:
```

```
-----
Version: 01.01.00.00 - Tue Dec 10 14:15:58 EST 1996
```

```
CLUSTER INFORMATION:
```

```
-----
Address..... 131.2.25.91
Number of target ports..... 2
FIN clean up count..... 4000
Connection FIN timeout..... 30
Active connection stale timer... 1500
```

```
PORT 23 INFORMATION:
```

```
-----
Maximum weight..... 20
Port mode..... NONE
Port type..... TCP
All up nodes are weight zero... FALSE
Total target nodes..... 2
Currently marked down..... 0
Servers providing service to this port:
Address: 131.2.25.93 Weight: 20 Count: 0
Active: 0 FIN 0 Status: up Saved Weight: -1
Address: 131.2.25.94 Weight: 20 Count: 0
Active: 0 FIN 0 Status: up Saved Weight: -1
```

```
PORT 80 INFORMATION:
```

```
-----
Maximum weight..... 20
Port type..... BOTH
Port mode..... NONE
All up nodes are weight zero... FALSE
Total target nodes..... 2
Currently marked down..... 0
Servers providing service to this port:
Address: 131.2.25.93 Weight: 20 Count: 0
Active: 0 FIN 0 Status: up Saved Weight: -1
Address: 131.2.25.94 Weight: 20 Count: 0
Active: 0 FIN 0 Status: up Saved Weight: -1
```

counter Obtiene el estado de todos los contadores.

Ejemplo:

```

status counter
Internal counters from executor:
-----
Total number of packets into executor..... 2684
Total packets for cluster processing (C)... 2684
Packets not addressed to a cluster(port)... 0

Cluster processing results:
-----
Errors..... 0
Discarded..... 0
Forward requested..... 2684
Forward requested..... 0
Forward discarded with error..... 0

Other processing problems:
-----
Total packets dropped (C)..... 0
  
```

manager Obtiene el estado del gestor.

Ejemplo:

```

status manager
Number of defined hosts... 2
Sensitivity..... 0%
Smoothing factor..... 2
Interval..... 3
Weights refresh cycle.... 4

Active connections gauge proportion..... 40%
New connections counter(delta) proportion... 38%
Advisor gauge proportion..... 20%
System Metric proportion..... 2%

Manager status requested.
  
```

port cluster-address port#

Obtiene el estado de un puerto específico, donde:

cluster-address

es la dirección IP del cluster.

port#

es el número de puerto en el cluster.

Ejemplo:

```

status port
Cluster Address [0.0.0.0]? 131.2.25.91
Port number [0]? 80

PORT 80 INFORMATION:
-----
Maximum weight..... 20
Port mode..... NONE
Port type..... BOTH
All up nodes are weight zero.... FALSE
Total target nodes..... 2
Currently marked down..... 0
Servers providing service to this port:
Address: 131.2.25.93 Weight: 20 Count: 12345 TCP Count: 10000 UDP count 2345
Active: 3431 FIN 3780 Complete 3431 Status: up Saved Weight: -1
Address: 131.2.25.94 Weight: 20 Count: 7890 Active: 2980 FIN 2390 Status: up
Saved Weight: -1
  
```

server address

Obtiene el estado de un servidor específico, donde *address* es la dirección IP del cluster al que pertenece el servidor.

Configuración de Network Dispatcher

Ejemplo:

```
status server
Cluster Address [0.0.0.0]? 131.2.25.91

PORT 23 INFORMATION:
-----
Maximum weight..... 20
Port mode..... NONE
Port type..... TCP
All up nodes are weight zero... FALSE
Total target nodes..... 2
Currently marked down..... 0
Servers providing service to this port:
Address: 131.2.25.93 Weight: 20 Count: 140 TCP Count: 100 UDP Count: 40
Active: 50 FIN 45 Complete 50 Status: up Saved Weight: -1
Address: 131.2.25.94 Weight: 20 Count: 250 TCP Count: 100 UDP Count: 40
Active: 60 FIN 54 Complete 50 Status: up Saved Weight: -1

PORT 80 INFORMATION:
-----
Maximum weight..... 20
Port mode..... NONE
Port type..... BOTH
All up nodes are weight zero... FALSE
Total target nodes..... 2
Currently marked down..... 0
Servers providing service to this port:
Address: 131.2.25.93 Weight: 20 Count: 12345 TCP Count: 10000 UDP Count: 2345
Active: 3431 FIN 3780 Complete 3431 Status: up Saved Weight: -1
Address: 131.2.25.94 Weight: 20 Count: 7890 TCP Count: 10000 UDP Count: 2345
Active: 2980 FIN 2390 Complete 3431 Status: up Saved Weight: -1
```

Switchover

Utilice el mandato **switchover** para obligar a un Network Dispatcher, que se ejecuta en modalidad de espera, a convertirse en el Network Dispatcher activo cuando la estrategia de conmutación sea manual. Es preciso entrar este mandato en el sistema principal que ejecuta el Network Dispatcher que está en la modalidad de espera.

Sintaxis:

switchover

Unquiesce

Utilice el mandato **unquiesce** para reiniciar una función heartbeat, manager o reach detenida previamente con el mandato **quiesce**.

Sintaxis:

```
unquiesce      hheartbeat
                  manager
                  reach
```

heartbeat *address*

Reinicia la vía de acceso para los mensajes Heartbeat, donde *address* es la dirección IP del Network Dispatcher remoto al que este Network Dispatcher está enviando mensajes Heartbeat.

Ejemplo:

```
unquiesce heartbeat
Remote Address [0.0.0.0]? 9.10.11.1
```

manager *address*

Reinicia el envío de peticiones de conexión al servidor especificado. *address* es la dirección IP del servidor.

Ejemplo:

```
unquiesce manager  
Server Address [0.0.0.0]? 20.21.22.15
```

reach *address*

Reinicia el sondeo que Network Dispatcher realiza en la dirección especificada para determinar si puede alcanzarse, donde *address* es la dirección IP que forma parte de los criterios de capacidad de alcance.

Ejemplo:

```
unquiesce reach  
Reach address [0.0.0.0]? 20.3.4.5
```

Configuración de Network Dispatcher

Configuración y supervisión de la Antememoria de IBM eNetwork Host On-Demand Client

La Antememoria de Host On-Demand Client permite a los clientes basados en Web conectar con las aplicaciones de sistema principal SNA que utilicen un programa de emulación de terminal basado en Java, que conecta al cliente con el sistema principal utilizando TN3270. Este soporte permite que un IBM 2216 actúe como un servidor TN3270E para colocar en antememoria la applet de emulación de terminal y enviarla a los navegadores de los clientes si la solicitan. La applet se recupera desde un Web Server la primera vez que la solicita un cliente, se guarda en la memoria y se pone a disposición de los clientes como respuesta a peticiones HTTP get de la applet.

Nota: Las características Antememoria de Host On-Demand Client y Antememoria de Web Server no pueden coexistir en una misma configuración.

Este capítulo describe cómo configurar la característica Antememoria de Host On-Demand Client y utilizar los mandatos de supervisión de Antememoria de Host On-Demand Client. Contiene:

- “Configuración de la Antememoria de Host On-Demand Client”
- “Acceso al entorno de configuración de la Antememoria de Host On-Demand Client” en la página 159
- “Mandatos de la Antememoria de Host On-Demand Client” en la página 159
- “Acceso al entorno de supervisión de la Antememoria de Host On-Demand Client” en la página 163
- “Mandatos de supervisión de la Antememoria de On-Demand Client” en la página 163.

Consulte “Visión general del gestor de control de antememoria externa” en la página 179 para obtener información acerca del uso del Gestor de control de antememoria externa, que funcionará con la Antememoria de Host On-Demand Client.

Configuración de la Antememoria de Host On-Demand Client

Es preciso utilizar la Antememoria de Host On-Demand Client con Network Dispatcher. Antes de utilizar la Antememoria de Host On-Demand Client por primera vez, debe realizar lo siguiente:

1. Acceder a Network Dispatcher en talk 6 desde el indicador Config> mediante el mandato **feature ndr**.
2. Habilitar el ejecutor
3. Añadir un cluster
4. Añadir un puerto
5. Añadir uno o más servidores.

Entonces puede utilizar los mandatos de configuración y supervisión para alterar el entorno de la Antememoria de Host On-Demand Client.

Configuración y supervisión de la Antememoria de Host On-Demand Client

Nota: Aunque los cambios en Network Dispatcher efectuados mediante Talk 6 modifican la configuración que se ejecuta actualmente, los cambios de la Antememoria de Host On-Demand Client no la modifican, a menos que se active de manera explícita a través del mandato **activate** en Talk 6, o mediante la característica Antememoria de HOD Client de Talk 5. La excepción es que, si el cluster/puerto de un Proxy HTTP se elimina mediante la característica NDR de Talk 6, esto hará que el proxy HTTP de la Antememoria de Host On-Demand Client se elimine también de la configuración que se ejecuta actualmente.

Ejemplo:

```
Config>f ndr
NDR Config>enable executor
NDR Config>add cluster
Cluster Address [0.0.0.0]? 113.3.1.10
FIN count [4000]?
FIN time out [30]?
Stale timer [1500]?
Cluster 113.3.1.10 has been added.
Fincount has been set to 4000 for cluster 113.3.1.10
Fintimeout has been set to 30 for cluster 113.3.1.10
Staletimer has been set to 1500 for cluster 113.3.1.10
NDR Config>add port
Cluster Address [0.0.0.0]? 113.3.1.10
Port number [80]? 80
Port type(tcp=1, udp=2, both=3) [3]?
Max. weight (0-100) [20]?
Only one pftp port per cluster allowed
Port mode (none=0, sticky=1 pftp=2 extcache=4 hod client cache=5) [0]? 5
Default server TCP connection timeout (Range 5-240 seconds) [120]?
Default client TCP connection timeout (Range 5-240 seconds) [120]?
Maximum partition size (1-4095 megabytes or 0 for no limit) [0]?
URL mask to identify Java applet [*.*.jar]?
    Default expiration time for Java applet
        (1-10080 minutes or 0 for no expiration) [60]?
Do you want to add a URL mask? [No]:

Host On-Demand Client Cache partition number 0 has been successfully created.
Requested port has been added to cluster 113.3.1.10
Port Mode has been set to hod for port 80 in cluster 113.3.1.10
Maxweight has been set to 20 for port 80 in cluster 113.3.1.10
Port Type has been set to Both for port 80 in cluster 113.3.1.10
NDR Config>exit
```

A continuación se listan los parámetros del ejemplo y sus descripciones.

cluster-address Especifica la dirección IP del cluster.

Nota: Se supone que las Direcciones IP de cluster se encuentran en la misma subred lógica que el direccionador de salto (direccionador IP) anterior.

Valores válidos: cualquier dirección IP válida

Valor por omisión: 0.0.0.0

FIN-count Especifica el número de conexiones que deben estar en estado FIN antes de que el ejecutor intente eliminar la información de conexión no utilizada de la base de datos de Network Dispatcher después de que haya transcurrido el tiempo indicado en *FIN-timeout* o *Stale-timer*.

Valores válidos: de 0 a 65535

Valor por omisión: 4000

Configuración y supervisión de la Antememoria de Host On-Demand Client

FIN-timeout	<p>Especifica el número de segundos que una conexión ha permanecido en el estado FIN, después de lo cual el ejecutor intenta eliminar la información de conexión no utilizada de la base de datos de Network Dispatcher.</p> <p>Valores válidos: de 0 a 65535</p> <p>Valor por omisión: 30</p>
Stale-timer	<p>Especifica el número de segundos que una conexión ha permanecido inactiva, después de lo cual el ejecutor intenta eliminar la información de la conexión de la base de datos de Network Dispatcher.</p> <p>Valores válidos: de 0 a 65535</p> <p>Valor por omisión: 1500</p>
port#	<p>Especifica el número de puerto del protocolo para este cluster.</p> <p>Valores válidos: 1 a 65535</p> <p>Valor por omisión: 80</p>
port-type	<p>Especifica los tipos de tráfico IP en los que se puede establecer el equilibrio de carga en seguridad. Los tipos soportados son:</p> <ul style="list-style-type: none">• 1 = TCP• 2 = UDP• 3 = ambos <p>Valores válidos: 1, 2, 3</p> <p>Valor por omisión: 3</p>
max-weight	<p>Especifica el peso máximo de los servidores en seguridad. Esto afecta al grado de diferencia que puede existir entre el número de peticiones que el ejecutor proporcionará a cada servidor.</p> <p>Valores válidos: 0 a 100</p> <p>Valor por omisión: 20</p>
port-mode	<p>Especifica si el puerto proveerá todas las peticiones de un único cliente a un único servidor (conocido como "sticky"), utilizará el ftp pasivo (pftp), proveerá una matriz de antememoria escalable externa (extcache), utilizará la Antememoria de Host On-Demand Client, o no utilizará ningún protocolo en particular en este cluster (none).</p> <p>Valores válidos: 0,1,2,4,5, donde:</p> <ul style="list-style-type: none">• 0 = none• 1 = sticky• 2 = pftp• 4 = extcache• 5 = hod client cache <p>Valor por omisión: 0</p>

Default server TCP connection timeout (Tiempo de espera de conexión TCP de servidor por omisión) Especifica el tiempo antes de que caduque una conexión de servidor.

Valores válidos: de 5 a 240 segundos

Valor por omisión: 120 segundos

Default client TCP connection timeout (Tiempo de espera de conexión TCP de cliente por omisión) Especifica el tiempo antes de que caduque una conexión de cliente.

Valores válidos: de 5 a 240 segundos

Valor por omisión: 120 segundos

Do you want to modify Host On-Demand Client Cache partition? (¿Desea modificar la partición de la Antememoria de Host On-Demand Client?) Permite modificar la configuración de la partición de la Antememoria de Host On-Demand Client.

Valores válidos: Yes o No

Valor por omisión: No

Maximum partition size (Tamaño máximo de partición) Especifica la cantidad máxima de memoria que va a asignarse a esta partición de Antememoria de Host On-Demand Client. Si este valor sobrepasa la cantidad de memoria disponible actualmente, se pasará por alto y no se impondrá ningún tamaño máximo de partición.

Valores válidos: de 1 a 4095 Megabytes ó 0 (sin máximo)

Valor por omisión: 0 (sin máximo)

URL mask to identify Java applets (Máscara de URL para identificar applets Java) Especifica la máscara de URL utilizada para identificar applets Java.

Valores válidos: cualquier máscara de URL

Valor por omisión: *.jar*

Default expiration time for Java applet (Tiempo de caducidad por omisión para applet Java) Especifica el tiempo de caducidad por omisión que se aplicará a las applets Java.

Valores válidos: 1 - 10080 minutos, ó 0 si no hay caducidad

Valor por omisión: 60

Do you want to add a URL mask? (¿Desea añadir una máscara de URL?) Especifica una nueva máscara de URL que se debe añadir a la Antememoria de Host On-Demand Client. Las máscaras de URL permiten al usuario incluir o excluir objetos individuales o grupos de objetos según su URL (Localizador de recursos universal).

Valores válidos: Yes o No

Valor por omisión: No

Los caracteres comodines pueden utilizarse al especificar una máscara de URL. Pueden utilizarse comodines al configurar Network Dispatcher para la Antememoria de Host On-Demand Client o al utilizar el mandato **add** o **modify url** del indicador HOD Client Cache. Los caracteres utilizados como comodines son * (asterisco) o #

(signo numérico). Pueden utilizarse comodines en cualquier posición como parte del URL.

El * no representa ningún carácter o bien todos los caracteres como parte de ese URL:

Ejemplo: *abc.html filtraría las siguientes máscaras de URL.

```
abc.html  
finabc.html  
defchtjqsprabc.html
```

representa cualquier carácter individual.

Ejemplo: ab#.html filtraría las siguientes máscaras de URL.

```
abc.html  
abf.html  
abo.html
```

Debe utilizar Network Dispatcher para configurar el cluster y el puerto iniciales para la característica Antememoria de Host On-Demand Client. Una vez que haya añadido el cluster y el puerto, configurando la *modalidad de puerto* como puerto de la Antememoria de Host On-Demand Client, podrá modificar y visualizar los parámetros de configuración de la Antememoria de Host On-Demand Client en el indicador HOD Client Cache Config>.

Consulte la página 130 para obtener información acerca de Network Dispatcher.

Acceso al entorno de configuración de la Antememoria de Host On-Demand Client

Para acceder al entorno de configuración de la Antememoria de Host On-Demand Client, entre el mandato **f hod client cache** en el indicador Config>.

```
Config> f h  
HOD Client Cache Config>
```

Mandatos de la Antememoria de Host On-Demand Client

Esta sección describe los mandatos de configuración de la Antememoria de Host On-Demand Client. La Tabla 17 en la página 160 lista los mandatos de configuración de Host On-Demand Client. Estos mandatos especifican los parámetros de la característica Antememoria de Host On-Demand Client. Para activar estos cambios, reinicie el direccionador.

Tabla 17. Resumen de los mandatos de configuración de la Antememoria de Host On-Demand Client

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxiv.
Activate	Activa la partición de la Antememoria de Host On-Demand Client, utilizando la configuración más reciente.
Add	Añade una máscara de URL.
Delete	Suprime una máscara de URL o una partición.
List	Lista la información de la Antememoria de Host On-Demand Client.
Modify	Modifica la información de la Antememoria de Host On-Demand Client.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiv.

Activate

Utilice el mandato **activate** para inicializar todas las particiones de la Antememoria de Host On-Demand Client, utilizando la configuración más reciente.

Sintaxis:

activate

Ejemplo:

```
HOD Client Cache Config>act ?
ACTIVATE ALL initializes the Host On-Demand Client Cache partition, using
the latest configuration.
If you want to keep the active configuration, use the
ENABLE PARTITION command.
```

Add

Utilice el mandato **add** para añadir una máscara de URL.

Sintaxis:

add urlmask

Ejemplo:

```
HOD Client Cache Config>add ur1
New URL mask []? *newmask*
Include or Exclude from HOD Client Cache (i or e) [i]? i
Set default expiration time? [No]: y
Default expiration time
(1-10080 minutes or 0 for no expiration) [0]? 60
The URL mask has been added to HOD Client Cache partition number 0.
```

Nota: Para añadir proxys y una partición, debe utilizar Network Dispatcher y ejecutar los mandatos **add port** o **set port**.

Delete

Utilice el mandato **delete** para suprimir una máscara de URL o la partición.

Sintaxis:

```
delete          partition
                urlmask
```

partition Suprime la partición de la Antememoria de Host On-Demand Client.

urlmask Nombre de la máscara de URL que debe suprimirse de la Antememoria de Host On-Demand Client.

Ejemplo:

```
HOD Client Cache Config>del part
HOD Client Cache partition number 0 has been deleted.
```

Ejemplo:

```
HOD Client Cache Config>delete url
URL masks defined : 1
  1: INCLUDE '*newmask*'
      Default expiration time: 60 minutes (1 hrs 0 mins)
URL mask number [1]?1
The URL mask for HOD Client Cache partition number 0 has been deleted.
```

Nota: Para suprimir un proxy, debe utilizar la característica Network Dispatcher y eliminar el puerto y/o cluster asociado, o bien cambiar la modalidad de puerto de el puerto de manera que no sea la Antememoria de Host On-Demand Client.

List

Utilice el mandato **list** para listar la información sobre la Antememoria de Host On-Demand Client.

Sintaxis:

```
list           all
                external
                partition
                proxy
                urlmask
```

all Lista la partición y todos los puertos, proxys y máscaras que están definidos en la Antememoria de Host On-Demand Client.

external Lista la información del Gestor de control de antememoria externa.

partition Lista la partición de la Antememoria de Host On-Demand Client.

proxy Lista los proxys de la Antememoria de Host On-Demand Client.

urlmask Lista las máscaras de URL de la Antememoria de Host On-Demand Client que se han definido.

Ejemplo: list all

```
HOD Client Cache Config>list all
Host On-Demand Client Cache Partition 0
  Cluster address 113.3.1.10, Port 80
```

```
1 Host On-Demand Client Cache partition defined.
```

Configuración y supervisión de la Antememoria de Host On-Demand Client

Ejemplo: list external

```
HOD Client Cache Config>list ext
External cache manager : Enabled
Port number           : 82
TCP timeout           : 120 seconds
```

Ejemplo: list partition

```
HOD Client Cache Config>list pa
Host On-Demand Client Cache Partition 0
Maximum partition size : Unlimited
URL mask to identify Java applets: '*.jar'
    Default expiration time for Java applet: 60
Associated proxies (cluster port): (113.3.1.10 80)

1 Host On-Demand Client Cache partition defined.
```

Ejemplo: list proxy

```
HOD Client Cache Config>li pro
1) Cluster address 113.3.1.10, Port 80, HOD Client Cache partition 0
HTTP proxy number [1]? 1
HTTP Proxy 1
HOD Client Cache Partition: 0
Cluster Address           : 113.3.1.10
Port Number               : 80
Server Connection Timeout : 120 seconds
Client Connection Timeout : 120 seconds
```

Ejemplo: list urlmask

```
HOD Client Cache Config>list url
URL masks defined : 1
1: INCLUDE '*newmask*'
    Default expiration time: 60 minutes (1 hrs 0 mins)
```

Modify

Utilice el mandato **modify** para modificar la información de configuración de la Antememoria de Host On-Demand Client.

Sintaxis:

```
modify          external
                  partition
                  proxy
                  urlmask
```

external Cambia las características del Gestor de control de antememoria externa.

partition Cambia las características de la partición de la Antememoria de Host On-Demand Client.

proxy Cambia las características de un proxy HTTP existente.

urlmask Cambia una máscara de URL existente.

Ejemplo: modify external

```
HOD Client Cache Config>mod ext
External cache manager port number (0 to disable) [82]? 83
TCP connection timeout (Range 5-240 seconds) [120]?
Do you want to modify the encryption key? [No]:
The external cache manager has been modified.
```

Ejemplo: modify partition

```
HOD Client Cache Config>modify partition
Maximum partition size (1-4095 megabytes or 0 for no limit) [0]? 2000
URL mask to identify Java applet [*.jar]?
    Default expiration time for Java applet
        (1-10080 minutes or 0 for no expiration) [60]?
Host On-Demand Client Cache partition number 0 has been modified.
```

Ejemplo: modify proxy

```
HOD Client Cache Config>mod proxy
1) Cluster address 113.3.1.10, Port 80, HOD Client Cache partition 0
HTTP proxy number [1]? 1
Default server TCP connection timeout (Range 5-240 seconds) [120]? 200
Default client TCP connection timeout (Range 5-240 seconds) [120]?
The HTTP proxy has been modified.
```

Ejemplo: modify url

```
HOD Client Cache Config>modify url
URL masks defined : 1
    1: INCLUDE '*newmask*'
        Default expiration time: No expiration
URL mask number [1]?
New URL mask [*newmask]?
Include or Exclude from HOD Client Cache (i or e) [i]?
Set default expiration time? [No]: y
Default expiration time
    (1-10080 minutes or 0 for no expiration) [0]? 60
URL mask number 1 has been modified.
```

Acceso al entorno de supervisión de la Antememoria de Host On-Demand Client

Para acceder al entorno de supervisión de la Antememoria de Host On-Demand Client, entre el mandato **f hod client cache** en el indicador de configuración t 5.

```
+f h
```

Mandatos de supervisión de la Antememoria de On-Demand Client

La Tabla 18 en la página 164 lista los mandatos de supervisión de la Antememoria de Host On-Demand Client.

Tabla 18. Resumen de mandatos de supervisión de la Antememoria de Host On-Demand Client

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxiv.
Activate	Activa la información de la Antememoria de Host On-Demand Client, utilizando la configuración más reciente.
Clear	Borra todos los objetos de la partición de la Antememoria de Host On-Demand Client, o borra las estadísticas de la Antememoria de Host On-Demand Client.
Enable	Habilita la partición de la Antememoria de Host On-Demand Client.
Delete	Suprime la partición, el proxy o la máscara de URL de la Antememoria de Host On-Demand Client.
Disable	Inhabilita la partición de la Antememoria de Host On-Demand Client.
List	Lista la información de la Antememoria de Host On-Demand Client.
Modify	Modifica la información de la Antememoria de Host On-Demand Client.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiv.

Activate

Utilice el mandato **activate** para activar la partición de la Antememoria de Host On-Demand Client o los proxys, o bien un proxy específico.

Sintaxis:

activate all
 external
 partition
 proxy

all Activa la partición de la Antememoria de Host On-Demand Client, todos los proxys definidos y el Gestor de control de antememoria externa definido.

external Activa el Gestor de control de antememoria externa.

partition Activa la partición de la Antememoria de Host On-Demand Client.

proxy Activa un proxy de la Antememoria de Host On-Demand Client.

Ejemplo: activate all

```
HOD Client Cache>act all
Host On-Demand Client Cache partition 0 must be disabled to reactivate it.
Do you wish to continue? [No]: y
```

Ejemplo: activate partition

```
HOD Client Cache>act pa
Host On-Demand Client Cache partition 0 must be disabled to reactivate it.
Do you wish to continue? [No]: y
Do you wish clear this partition? [No]: y
Do you wish to enable this partition? [Yes]: y
```

Ejemplo: activate proxy


```
HOD Client Cache>activate pr
  1) Cluster address 113.3.1.10, Port 80, HOD Client Cache partition 0
Enter proxy number: [1]? 1
You are trying to activate an existing proxy.
Doing this will cause the proxy to be terminated before
being reactivated.
Do you wish to continue? [No]: y
```

Clear

Utilice el mandato **clear** para borrar todos los objetos de la partición de la Antememoria de Host On-Demand Client, o para borrar estadísticas.

Nota: El borrado de los objetos de la partición no borra las estadísticas de la partición.

Sintaxis:

```
clear           partition
                  statistics
```

partition Borra todos los objetos de la partición.

statistics Borra las estadísticas existentes de la partición.

Ejemplo: clear partition

```
HOD Client Cache>clear pa
HOD Client Cache partition 0 must be disabled to clear its contents.
Do you wish to continue? [No]: y
Do you wish to enable this partition? [Yes]: y
```

Enable

Utilice el mandato **enable** para habilitar la partición de la Antememoria de Host On-Demand Client.

Sintaxis:

```
enable          partition
```

Ejemplo:

```
HOD Client Cache>enable partition
```

Delete

Utilice el mandato **delete** para suprimir la partición de la Antememoria de Host On-Demand Client.

Sintaxis:

```
delete          partition
```

partition Suprime la partición de la Antememoria de Host On-Demand Client.

Ejemplo: delete partition

```
HOD Client Cache>delete partition
WARNING: This will delete partition and free all memory!
Do you wish to continue? [No] : yes
HOD Client Cache>
```

Disable

Utilice el mandato **disable** para inhabilitar la partición de la Antememoria de Host On-Demand Client.

Sintaxis:

disable partition

Ejemplo:

```
HOD Client Cache>disable partition
```

List

Utilice el mandato **list** para visualizar la información para la partición de la Antememoria de Host On-Demand Client, todas las políticas y los proxys, o bien una política o un proxy específico.

Sintaxis:

list all
 delete
 depend
 external
 item
 partition
 policy
 proxy

- all** Lista la partición de la Antememoria de Host On-Demand Client, todas las políticas y todos los proxys.
- delete** Lista los 100 últimos elementos suprimidos de la partición de la Antememoria de Host On-Demand Client.
- depend** Lista la tabla de dependencias de la partición.
- external** Lista la información del Gestor de control de antememoria externa.
- item** Lista los elementos que existen actualmente en la partición de la Antememoria de Host On-Demand Client.
- partition** Lista la información sobre la partición de la Antememoria de Host On-Demand Client.
- policy** Lista la información sobre la política de la Antememoria de Host On-Demand Client.
- proxy** Lista la información sobre proxys de la Antememoria de Host On-Demand Client.

Ejemplo: list all

```
HOD Client Cache>list all
HOD Client Cache Partition 0                    Status: Enabled
                          Cluster address: 113.3.1.10 Port 80
1 partition(s) active.
External Cache Manager Port: 83
                          Connection timeout: 120 seconds
```

Ejemplo: list delete

```
HOD Client Cache>list delete
```

```
Delete Table
URL string -- hit count
=====
'/abc.html' -- 4
'/soccer.html' -- 2
'/tennis.html' -- 1
'/curling.html' -- 3
```

Ejemplo: list dependency

```
HOD Client Cache>list depend
Dependency table for Partition 0
```

```
-----
dep: tennis_info
    count of URLs: 2
    URLs:
        tennis_roster.html
        tennis_schedule.html
dep: soccer_info
    count of URLs: 2
    URLs:
        soccer_roster.html
        soccer_schedule.html
dep: schedule
    count of URLs: 2
    URLs:
        tennis_schedule.html
        soccer_schedule.html
```

Ejemplo: list external

```
HOD Client Cache>list external
External Cache Manager Port: 83
Connection timeout: 120 seconds
Current number of connections: 0
```

Ejemplo: list item

```
HOD Client Cache>list item
```

```
Current number of items: 5
URL String -- hit count
=====
'/' -- 2
'/file5k.html' -- 1
'/file4k.html' -- 1
'/file2k.html' -- 3
'/file1k.html' -- 1
```

Ejemplo: list partition

```
HOD Client Cache>list partition
HOD Client Cache Partition 0          Status: Enabled
      Cluster address: 113.3.1.10, Port 80
Partition size: Current - 0 bytes Highest - 0 bytes Maximum - Unlimited
Number of objects: Current - 0 Highest - 0 Maximum - Unlimited
Maximum object size: Unlimited
HOD Client Cache purge interval : 600 minute(s)
Hit ratio: 0%
Total number of hits: 0
Total number of misses: 0
Object Excluded (Object too large): 0
                (Object expired): 0
                (DONT CACHE header): 0
                (URL Mask excluded): 0
                (Image excluded): 0
                (Static object excluded): 0
                (Dynamic object excluded): 0
                (Cache disabled): 0
Objects explicitly Included: 0
Total number of purged objects: 0
Purged objects (Cache full): 0
                (Object stale): 0
                (Purged by user): 0
                (Invalidation): 0
```

Ejemplo: list policy

```
HOD Client Cache>list policy
URL mask to identify Java Applets: *.jar
      Default lifetime: 60 minute(s)
URL masks defined:
  1: INCLUDE *newmask*
      Default expiration time: 60 minutes (1 hrs 0 mins)
```

Ejemplo: list proxy

```
HOD Client Cache>list proxy
  1) Cluster address 113.3.1.10, Port 80, HOD Client Cache Partition 0
Enter proxy number: [1]? 1
Proxy 1: assigned to HOD Client Cache partition 0
Cluster address: 113.3.1.10 Port number: 80
Server Connection Timeout: 120 seconds
Client Connection Timeout: 120 seconds
Client connections: 0 current / 0 at highest point
Server connections: 0 current / 0 at highest point
Total cache hits: 0
Total cache misses: 0
Cache misses (object not in cache): 0
                (unsupported method): 0
                (can't send response): 0
                (non-cached request): 0
```

Modify

Utilice el mandato **modify** para modificar el Gestor de control de antememoria externa.

Sintaxis:

```
modify          external
```

Ejemplo: modify external

```
HOD Client Cache Config>mod ext
External cache manager port number (0 to disable) [83]? 82
TCP connection timeout (Range 5-240 seconds) [120]?
Do you want to modify the encryption key? [No]: n
```

Utilización de la Antememoria del servidor de la web

Este capítulo describe la característica Antememoria del servidor de la web del 2216. Contiene las siguientes secciones:

- “Visión general de la Antememoria del servidor de la web”
- “Utilización del Proxy HTTP” en la página 174
- “Antememoria escalable de alta disponibilidad” en la página 176
- “Visión general del gestor de control de antememoria externa” en la página 179.

Visión general de la Antememoria del servidor de la web

El Función de colocación en antememoria del servidor de la web almacena las páginas web solicitadas con mayor frecuencia para recuperarlas rápidamente. El Función de colocación en antememoria del servidor de la web mantiene los elementos solicitados con frecuencia más cerca de los clientes; así se liberan recursos del servidor que se están utilizando para las conexiones para servir archivos y establecer comunicaciones. Antememoria del servidor de la web de 2216 proporciona un acceso de alta velocidad a las páginas web, al tiempo que reduce la actividad general de las comunicaciones del sistema principal. 2216 Antememoria del servidor de la web:

- Almacena las páginas web estáticas que no están protegidas
- Proporciona acceso a la antememoria a los clientes y servidores HTTP
- Permite la definición de usuario de las políticas de llenado e invalidación de antememoria
- Utiliza la función Network Dispatcher para realizar el equilibrio de la carga de trabajo entre los servidores y proporcionar la posibilidad de antememoria de copia de seguridad
- Proporciona una plataforma para las futuras funciones de antememoria dirigidas por el servidor.

Nota: Las características Antememoria de Web Server y Antememoria de Host On-Demand Client no pueden coexistir en una misma configuración.

Todas las interfaces de red de 2216 que dan soporte a la conectividad TCP/IP, dan soporte también a la conectividad entre Antememoria del servidor de la web, servidores HTTP y clientes.

La Figura 10 en la página 170 muestra cómo funciona Network Dispatcher sin el Función de colocación en antememoria del servidor de la web.

Utilización de la Antememoria del servidor de la web

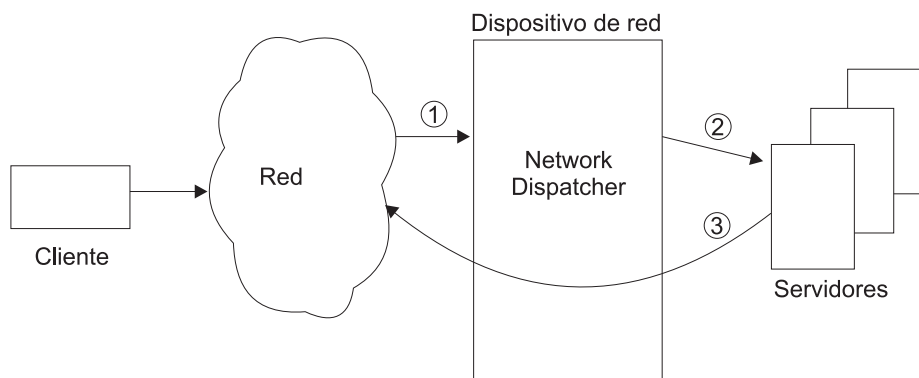


Figura 10. Network Dispatcher sin Antememoria del servidor de la web

1. Llega la petición para la dirección del cluster
2. Network Dispatcher reenvía la petición a los servidores
3. El servidor devuelve su respuesta al cliente.

La Figura 11 muestra cómo funciona Network Dispatcher sin el Función de colocación en antememoria del servidor de la web y la página solicitada no está almacenada en la antememoria. El Función de colocación en antememoria del servidor de la web carga la respuesta en la antememoria si las políticas lo permiten.

Consulte “Utilización del Proxy HTTP” en la página 174 para obtener información acerca del Proxy HTTP.

Una partición es una división de la memoria nuclear de la antememoria. Cada partición de la antememoria es independiente y permite que el dispositivo dé soporte a varios clusters.

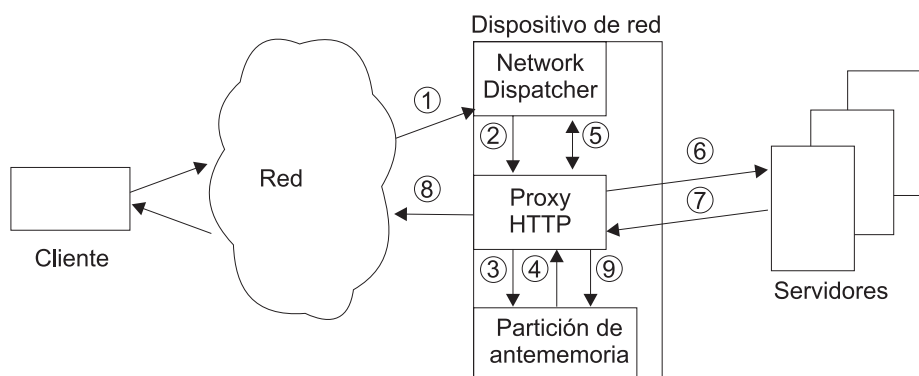


Figura 11. Network Dispatcher con Antememoria del servidor de la web y sin entradas en la antememoria

1. Llega la petición para la dirección del cluster
2. Network Dispatcher reenvía la petición al Proxy HTTP, si está activo
3. El Proxy HTTP consulta la partición de la antememoria
4. El Proxy HTTP no encuentra la página solicitada en la partición de la antememoria
5. El Proxy HTTP obtiene información sobre el servidor de Network Dispatcher si es necesaria para establecer una nueva conexión

6. El Proxy HTTP reenvía la petición al servidor. (Para la conexión TCP, la dirección IP de origen es la dirección de la interfaz de red del 2216. La dirección IP de destino es la dirección IP de la interfaz de servidor.)
7. El servidor devuelve su respuesta al Proxy HTTP
8. El Proxy HTTP envía la respuesta al cliente
9. El Proxy HTTP carga la respuesta en la partición de la antememoria si las políticas lo permiten.

La Figura 12 muestra cómo funciona Network Dispatcher con el Función de colocación en antememoria del servidor de la web cuando la página solicitada está almacenada en la antememoria.

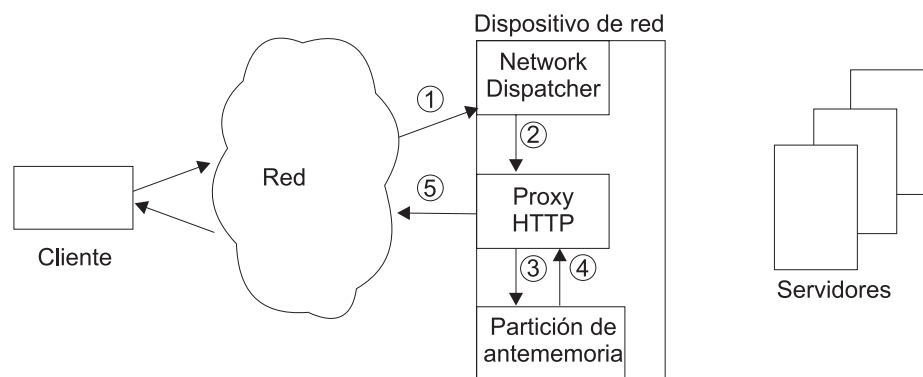


Figura 12. Network Dispatcher con Antememoria del servidor de la web y con entradas en la antememoria

1. Llega la petición para la dirección del cluster
2. Network Dispatcher reenvía la petición al Proxy HTTP
3. El Proxy HTTP consulta la partición de la antememoria
4. El Proxy HTTP encuentra la página solicitada en la partición de la antememoria
5. El Proxy HTTP devuelve la respuesta al cliente.

Colocación en la antememoria

Antememoria del servidor de la web del 2216 tiene:

Colocación en antememoria de páginas web

El 2216 puede almacenar en la antememoria los objetos solicitados desde el servidor. Este tipo de colocación en antememoria se denomina "transparente". Puede utilizar `talk 6` para habilitar o inhabilitar la colocación en antememoria transparente para una partición.

La colocación en antememoria alternativa a la transparente (automático) es la colocación manual. En este caso, un agente externo utiliza el gestor de antememoria para colocar en la antememoria una página web. Para obtener información acerca de la colocación en antememoria externa, consulte "Visión general del gestor de control de antememoria externa" en la página 179.

Los objetos sobrantes que han quedado colocados en la antememoria se suprimen automáticamente. Antememoria del ser-

vidor de la web del 2216 da soporte a los servidores y a los clientes HTTP 1.0 y 1.1.

Políticas de antememoria flexibles

Permite especificar a los usuarios si ciertas clases amplias de objetos web (imágenes, páginas estáticas que no son imágenes o páginas dinámicas) deben colocarse en la antememoria. Puede especificar el tamaño máximo de los objetos y de las particiones de la antememoria. Además, los usuarios pueden especificar máscaras de URL para incluir o excluir explícitamente las clases de objetos web como sea apropiado para su entorno.

Diagrama de flujo de las políticas de colocación en antememoria transparente:

1. ¿Están habilitadas la colocación en antememoria y la colocación en antememoria transparente?
 - No - El objeto no se coloca en la antememoria.
 - Sí - Continuar con la comprobación siguiente.
2. ¿Se encuentra el tamaño del objeto dentro del tamaño máximo establecido para el objeto?
 - No - El objeto no se coloca en la antememoria.
 - Sí - Continuar con la comprobación siguiente.
3. ¿Ha caducado el objeto?
 - No - Continuar con la comprobación siguiente.
 - Sí - El objeto no se coloca en la antememoria.
4. ¿Deben utilizarse cabeceras HTTP y se ha utilizado una de las cabeceras HTTP?

Nota: La cabecera HTTP utilizada es la cabecera Cache-Control con las directrices DO o DONT.

- a. No - ¿No deben utilizarse cabeceras HTTP o no hay ninguna cabecera en el objeto?
 - 1) ¿Está el URL excluido por una máscara de exclusión?
 - Sí - El objeto no se coloca en la antememoria.
 - No - Continuar con la comprobación siguiente.
 - 2) ¿Está el URL incluido mediante una máscara de inclusión?
 - Sí - Vaya al paso 5 en la página 173.
 - No - Continuar con la comprobación siguiente.
 - 3) ¿Se trata de un objeto dinámico?
 - No - Continuar con la comprobación siguiente.
 - Sí - El objeto es dinámico.
 1. ¿Se pueden colocar los objetos dinámicos en la antememoria?
 - Sí - Continuar con la comprobación siguiente.

Utilización de la Antememoria del servidor de la web

— No - El objeto no se coloca en la antememoria.

4) ¿El objeto es una imagen (.jpg o .gif)?

- No - Continuar con la comprobación siguiente.
- Sí - El objeto es una imagen.

1. ¿Las imágenes pueden colocarse en la antememoria?

— Sí - Continuar con la comprobación siguiente.

— No - El objeto no se coloca en la antememoria.

5) ¿El objeto es un archivo estático que no es una imagen?

- No - Continuar con la comprobación siguiente.
- Sí - El objeto es un archivo estático que no es una imagen.

1. ¿Se pueden colocar en la antememoria los archivos estáticos que no son imágenes?

— Sí - Continuar con la comprobación siguiente.

— No - El objeto no se coloca en la antememoria.

b. Sí - ¿Se utilizan cabeceras HTTP y el objeto incluye una cabecera de control de antememoria?

1) ¿Las cabeceras HTTP indican la antememoria "DO"?

- a) No - El objeto no se coloca en la antememoria.
- b) Sí - Continuar con la comprobación siguiente.

5. ¿Existe espacio en la partición para el objeto?

Nota: Se eliminarán los objetos utilizados en la fecha menos reciente para crear espacio libre para el objeto.

- No - El objeto no se coloca en la antememoria.
- Sí - El objeto se coloca en la antememoria.

Soporte de varias antememorias independientes

Da soporte a un máximo de 16 particiones, permitiendo que un único 2216 proporcione servicios de antememoria independientes para varios clusters. Las particiones de antememoria son totalmente independientes. Cada partición de antememoria mantiene su propio contenido y sus políticas.

Plena conectividad de servidor TCP/IP

Comunica con servidores y clientes a través de todas las interfaces de red de 2216 que dan soporte al conjunto de protocolos TCP/IP.

Equilibrio de carga en los servidores de programas de fondo (a través de Network Dispatcher)

Utiliza Network Dispatcher para definir grupos de servidores y equilibrar la carga entre los servidores para acelerar la consulta de las páginas web que no se encuentren en la antememoria.

Soporte de antememoria de copia de seguridad

Permite a los usuarios definir un segundo 2216 como antememoria del servidor de copia de seguridad. La antememoria del servidor de copia de seguridad puede operar como copia de seguridad "fría" mediante la función de Alta disponibilidad de Network Dispatcher; consulte "Alta disponibilidad para Network Dispatcher" en la página 109 para obtener más información.

Nota: La antememoria de servidor de copia de seguridad se encuentra vacía. Debe volver a llenar la antememoria de servidor de copia de seguridad mediante la colocación en antememoria transparente (por ejemplo: peticiones de URL) o mediante la función del gestor de control de antememoria externa para forzar la colocación de las páginas en la antememoria.

Utilización del Proxy HTTP

Puede haber más de un Proxy HTTP en el 2216. Cada uno de ellos representa una dirección/puerto de clusters que realiza la colocación en antememoria. Puede haber varios proxys HTTP que utilicen una partición de antememoria.

El Proxy HTTP gestiona las peticiones recibidas de los clientes e intenta satisfacerlas desde su partición de antememoria. Si el Proxy HTTP puede satisfacer la petición, responde al cliente. Si el Proxy HTTP no puede satisfacer la petición, abre una conexión TCP con un servidor intentando satisfacer la petición. Cuando el servidor responde a la petición del Proxy HTTP, éste reenvía la respuesta del servidor al cliente. El Proxy HTTP también comprueba si la respuesta del cliente se debe colocar en la antememoria. Si se debe colocar en la antememoria, el Proxy HTTP lo pasará a la partición de la antememoria.

El Proxy HTTP gestiona las conexiones utilizando las siguientes directrices.

- El Proxy HTTP sólo intentará satisfacer las peticiones de método GET y HEAD de la antememoria. Todas las demás peticiones se enviarán sin modificaciones, a través de una conexión TCP, al servidor emparejado con la conexión TCP del cliente. Si no hay una conexión TCP emparejada con la conexión TCP del cliente, se abrirá una conexión TCP nueva en el servidor y se emparejará con la conexión TCP con el cliente.
- Todos los mensajes de las peticiones de método GET y HEAD que no se puedan satisfacer desde la partición de la antememoria se enviarán al servidor sin sufrir modificaciones a través de la conexión TCP.
- Todas las respuestas se devolverán al cliente, a través de la conexión TCP, sin efectuar modificaciones respecto a lo enviado por el servidor.
- Sólo se pueden colocar en la antememoria las respuestas del método GET. Todas las demás respuestas se consideran que no pueden colocarse en la antememoria. Las respuestas GET sólo se colocan en la antememoria si el estado de la respuesta es aceptable y la respuesta GET, junto con las políticas de colocación en antememoria para la partición, permite dicha colocación.
 - Sólo se colocarán en la antememoria las respuestas que tengan uno de los códigos de estado siguientes. El Proxy HTTP no permitirá que las cabeceras HTTP prevalezcan sobre esto.

Códigos de estado:

- 200 (bien)
 - 203 (sin autoridad)
 - 300 (múltiples opciones)
 - 301 (movido de manera permanente)
 - 410 (desaparecido)
- Cuando se utilizan cabeceras HTTP en la petición GET, sólo la cabecera de petición If-Modified-Since estará implicada en determinar si una entrada de la antememoria puede satisfacer la petición. No se utilizará ninguna otra cabecera condicional. La Antememoria del servidor de la web no usará códigos de entidad para determinar si puede utilizarse en una respuesta una entidad colocada en la antememoria.
 - Se pasan por alto las directrices de cabecera Cache-Control sobre las peticiones. Si la entidad no se encuentra en la partición de la antememoria, la petición se pasará al servidor.
Nota: La Antememoria del servidor de la web es una extensión del servidor y, por lo tanto, no utiliza la cabecera Cache-Control como las antememorias del Proxy HTTP.
 - Las directrices de cabecera de antememoria "do" y "dont" están soportadas en las respuestas. Todas las demás directrices se pasan por alto. Las directrices "do" y "dont" son nuevas y el servidor puede utilizarlas para indicar a Antememoria del servidor de la web que almacene la entidad en la antememoria o no.
Nota: Antememoria del servidor de la web es una extensión del servidor y, por lo tanto, no utiliza la cabecera Cache-Control como las antememorias del Proxy HTTP.
 - El Proxy HTTP intenta satisfacer peticiones GET parciales de la antememoria. No obstante, las respuestas GET parciales no se colocan en la antememoria.
Nota: Si una petición GET parcial tiene más de diez rangos, se devolverá toda la respuesta.
 - La cabecera Host se pasará por alto en todos los mensajes HTTP, dado que todas las peticiones entrantes deben dirigirse al mismo cluster del servidor.
 - El Proxy HTTP da soporte a conexiones HTTP permanentes.
Nota: Si una conexión permanente proviene de un cliente de nivel HTTP 1.0 y se devuelve la respuesta de la antememoria, añadirá una cabecera Connection basada en la petición. Por ejemplo, si el cliente desea una conexión prolongada, mantendrá este tipo de conexión.
 - El Proxy HTTP no utilizará la antememoria para las peticiones que contengan la cabecera Authorization. No se colocará en la antememoria una respuesta a semejante petición. Tampoco se colocará en la antememoria una cabecera Proxy-Authorization.
 - El Proxy HTTP podrá conmutar al funcionamiento de túnel para una conexión HTTP, si encuentra problemas al analizar una petición o una respuesta en una conexión HTTP. El funcionamiento de túnel detiene todo tipo de análisis de mensajes y reenviará todas las peticiones del cliente al servidor y todas las respuestas del servidor al cliente.

Utilización de la Antememoria del servidor de la web

- Si la partición de la antememoria está inhabilitada, todas las conexiones de cliente actuales y nuevas se reenvían directamente al servidor de fondo.
- Si la partición de la antememoria está habilitada, la antememoria procesa todas las conexiones de cliente nuevas. Las conexiones de cliente existente seguirán reenviando las peticiones directamente al servidor de fondo.

Antememoria escalable de alta disponibilidad

La Antememoria escalable de alta disponibilidad permite que un grupo de antememorias de Web Server conectadas funcionen como una única antememoria de gran tamaño. El número máximo de antememorias que puede haber en un grupo es de dieciséis. Una anomalía en un miembro de la antememoria reduce la cantidad total de memoria disponible para la colocación en la antememoria en lugar de finalizar todas las funciones de antememoria. Vea un ejemplo de configuración en la Figura 9 en la página 123.

Las antememorias individuales componen el espacio total de la antememoria. Si una antememoria deja de funcionar, las páginas entrantes se seguirán colocando en las antememorias de trabajo restantes.

Las páginas web entrantes se colocan en las antememorias del grupo. Se distribuyen entre las antememorias disponibles de manera equitativa. Cada antememoria del grupo mantiene una tabla que hace un seguimiento del número de antememorias que pueden alcanzarse en el grupo y sus direcciones IP. Las tablas son idénticas para todas las antememorias de un grupo. Las tablas se utilizan junto con un algoritmo CARP (Protocolo de rutina de matriz de antememoria) para determinar qué antememoria posee un URL determinado. La información de la tabla procede del dispositivo Network Dispatcher y, de forma indirecta, de las antememorias que utilizan el consejero HTTP para hacer un seguimiento del estado de las Antememorias de Web Server del grupo. En las figuras siguientes se muestran las condiciones necesarias para localizar un URL mediante SHAC.

La Figura 13 muestra la petición de Network Dispatcher que se ha encontrado en la primera antememoria que ha recibido la petición.

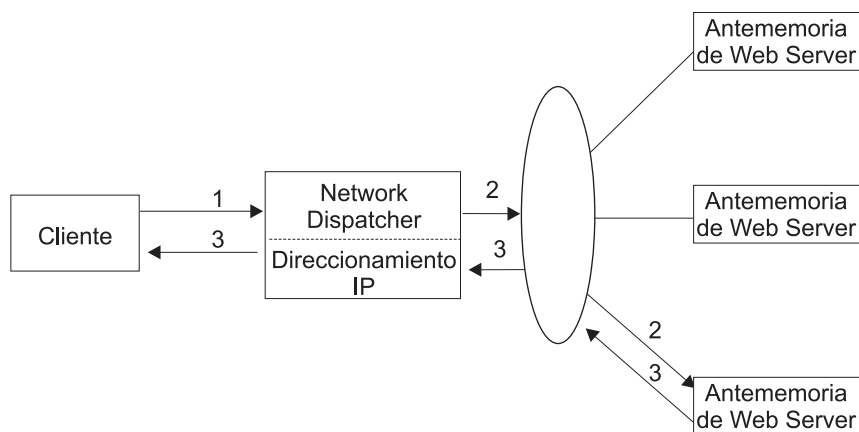


Figura 13. Petición de antememoria encontrada

1. De un cliente llega una petición HTTP de una página web a Network Dispatcher.

2. Network Dispatcher reenvía la petición a una de las Antememorias de Web Server. La antememoria recibe la petición y ve que contiene la página web.
3. La antememoria envía la página web directamente al cliente, ignorando a Network Dispatcher.

La Figura 14 muestra una petición no encontrada en la primera antememoria que ha recibido la petición de Network Dispatcher y el algoritmo CARP indica que otra antememoria posee el URL.

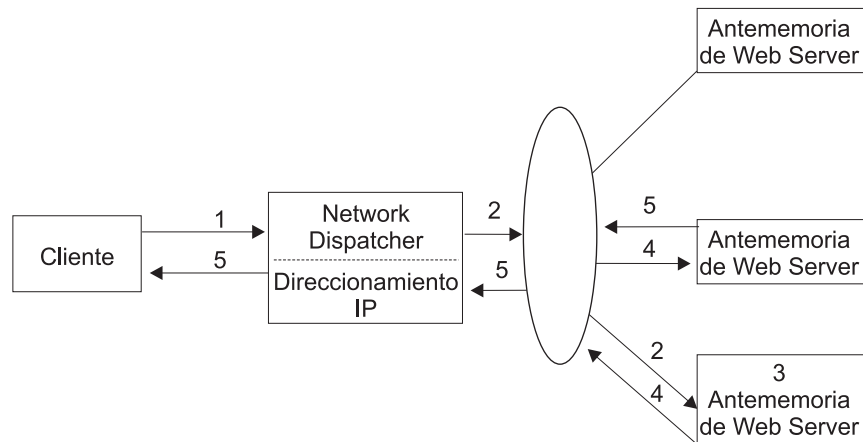


Figura 14. Petición reenviada a la antememoria responsable

1. De un cliente llega una petición HTTP de una página web a Network Dispatcher.
2. Network Dispatcher reenvía la petición a una de las Antememorias de Web Server.
3. La antememoria recibe la petición y no encuentra la página web en su antememoria. A continuación, la antememoria utiliza un algoritmo para localizar la antememoria responsable de la página web.
4. Posteriormente, la petición se reenvía a la antememoria responsable de esa página web.
5. La antememoria responsable de la página web recibe la petición, encuentra la página web y envía la página web al cliente.

La Figura 15 en la página 178 muestra una petición no encontrada en la antememoria que ha recibido la petición de Network Dispatcher, pero el algoritmo CARP indica que la antememoria es responsable del URL.

Utilización de la Antememoria del servidor de la web

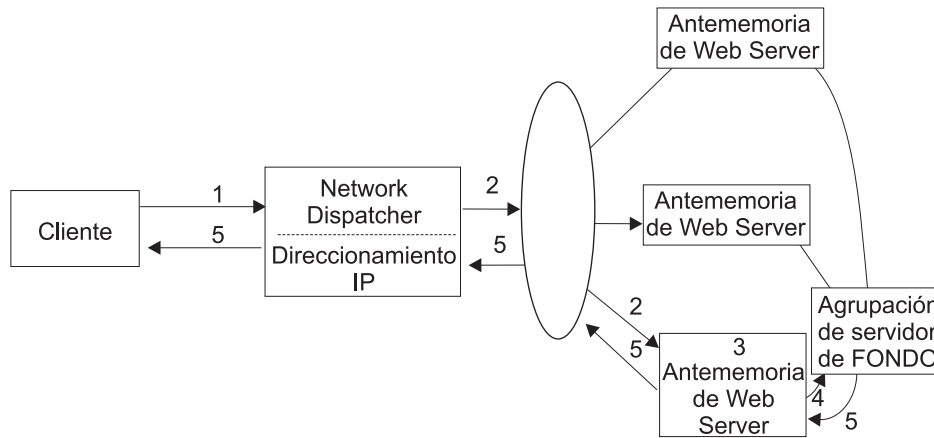


Figura 15. Petición reenviada al servidor de fondo

1. De un cliente llega una petición HTTP de una página web a Network Dispatcher.
2. Network Dispatcher reenvía la petición a una de las Antememorias de Web Server.
3. La antememoria recibe la petición y no encuentra la página web en su antememoria. La antememoria utiliza un algoritmo para determinar que es responsable de la página web.
4. La antememoria envía la petición al servidor de fondo.
5. El servidor de fondo encuentra la página web, la cual se devuelve al cliente a través de la antememoria responsable de la misma. Se colocará en la antememoria si ésta se ha configurado para almacenar esta página. Consulte “Configuración y supervisión de la Antememoria del servidor de la web” en la página 207 para obtener información sobre configuración.

La Figura 16 muestra una petición que no se encuentra en ninguna antememoria del grupo de antememorias.

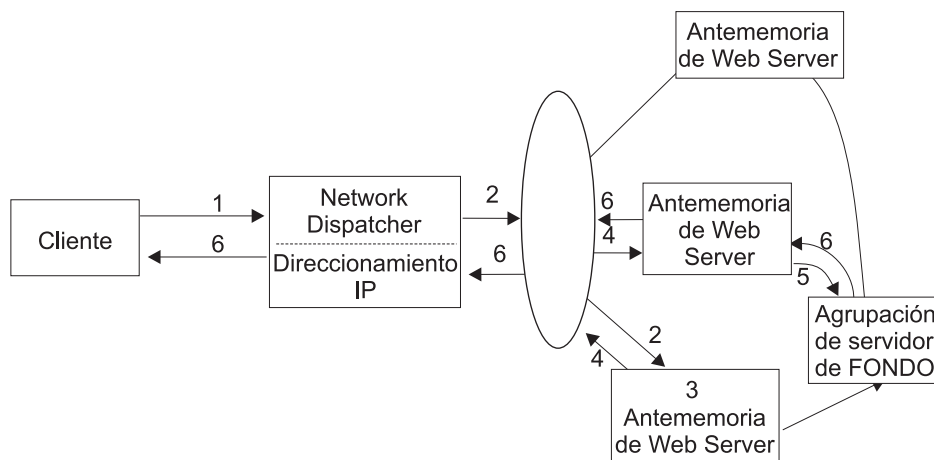


Figura 16. Petición reenviada a la antememoria responsable y no encontrada

1. De un cliente llega una petición HTTP de una página web a Network Dispatcher.

2. Network Dispatcher reenvía la petición a una de las Antememorias de Web Server.
3. La antememoria recibe la petición y no encuentra la página web en su antememoria. A continuación, la antememoria utiliza un algoritmo para localizar la antememoria responsable de la página web. Posteriormente, la petición se reenvía a la antememoria responsable de esa página web.
4. La antememoria responsable de la página web recibe la petición y no encuentra la página web.
5. La antememoria responsable de la página web envía la petición a la agrupación de servidor de fondo.
6. El servidor de fondo encuentra la página web, la cual se devuelve al cliente a través de la antememoria responsable de la misma. Se colocará en la antememoria si ésta se ha configurado para almacenar esta página. Consulte “Configuración y supervisión de la Antememoria del servidor de la web” en la página 207 para obtener información sobre configuración.

Visión general del gestor de control de antememoria externa

El Gestor de control de antememoria externa permite que los Web Servers tengan la capacidad de controlar la Antememoria de Web Server y la Antememoria de Host On-Demand Client. Este control se realiza mediante un puerto definido por el usuario para el Gestor de control de antememoria externa (ECCM). El ECCM acepta las conexiones y procesa los mandatos destinados a una partición a través de este puerto. Los mandatos utilizan el Protocolo de control de antememoria externa (ECCP). El ECCP utiliza formatos de vector/subvector para enviar mandatos de petición y de respuesta.

Un vector de mandato puede solicitar varias funciones mediante varios subvectores. Cada subvector representa una función nueva. El vector de mandato indica a qué partición de antememoria se aplicarán los mandatos, especificando la dirección del cluster y el puerto de un proxy definido en dicha partición.

ECCP da soporte a las funciones siguientes:

- Añadir/Suprimir un objeto a/de una partición de antememoria
- Habilitar/Inhabilitar una partición de antememoria
- Modificar/Listar las políticas de una partición de antememoria
- Borrar/Listar las estadísticas de una partición de antememoria
- Borrar una partición de antememoria (eliminar todos los objetos de una partición de antememoria)
- Consultar la partición de antememoria (buscar un objeto determinado)
- Añadir/Suprimir/Listar/Borrar las máscaras de URL de una partición de antememoria
- Modificar/Listar la tabla de dependencias
- Invalidar objetos mediante dependencias.

Tabla de dependencias

El Gestor de control de antememoria externa le permite crear una tabla de dependencias para cada partición de antememoria. Esta tabla resulta especialmente útil cuando se trabaja con objetos dinámicos en la antememoria.

Nota: La colocación en antememoria de objetos dinámicos exige que los objetos se actualicen cuando se modifique la información a partir de la cual se crearon.

La información necesaria para construir la tabla de dependencias debe pasarse a la partición de antememoria mediante la interfaz del Gestor de control de antememoria externa.

La tabla de dependencias proporciona la capacidad de asignar una serie de dependencias a un objeto de URL (una página web colocada en antememoria). Estas dependencias se almacenan en tablas de dependencias en la Antememoria de Web Server mediante la interfaz del Gestor de control de antememoria externa. La tabla de dependencias se utiliza para invalidar objetos en la partición de antememoria que tengan esta dependencia cuando se modifique el origen del objeto. Si careciera de una tabla de dependencias, tendría que enviar un mandato de supresión para cada objeto que debiera suprimirse.

Ejemplo: Las tres bases de datos siguientes contienen diversos objetos.

basedatos1	basedatos2	basedatos3
-----	-----	-----
objeto_a	objeto_a	objeto_b
objeto_b	objeto_c	objeto_e
objeto_c	objeto_d	

Suponga que todas las páginas desde objeto_a hasta objeto_e se encuentran en la antememoria. Si se modifica basedatos2, puede enviar (a través de la interfaz del Gestor de control de antememoria) un mandato **invalid dependency basedatos2**. La antememoria de Web Server suprimirá objeto_a, objeto_c y objeto_d de la partición de antememoria.

Nota: No es necesario que un objeto esté en la partición de antememoria para poder estar en la tabla de dependencias.

Autenticación del Gestor de control de antememoria externa

El Gestor de control de antememoria externa permite controlar el acceso de los usuarios. Esto se consigue obligando a las conexiones entrantes que tengan un ID de usuario y una contraseña. El ID de usuario y la contraseña están vinculados al ID de usuario y la contraseña de conexión. Si el dispositivo está protegido con contraseña y la conexión entrante no tiene ID de usuario y contraseña, o éstos no son válidos, se devolverá una respuesta de error de autenticación y se cerrará la conexión. Si el ID de usuario y la contraseña son válidos, el usuario podrá enviar mandatos a través de esta interfaz.

Seguridad

La seguridad proporciona una manera de autenticar el usuario de ECCP. Pueden configurarse cuatro tipos de autenticación (RADIUS, TACACS, local o ninguna). No se proporciona cifrado de datos. Cada mecanismo de autenticación (salvo que se determine que no hay ninguno) requiere un ID de usuario y una contraseña asociada. Esta información se pasa al 2216 mediante los vectores de autenticación. Tanto el ID de usuario como la contraseña pueden tener de 1 a 8 bytes. Es preciso

cifrar la contraseña que se pasa en la conexión de Control de antememoria externa, mediante el cifrado DES. También se pasa el número generador aleatorio de 8 bytes que se utiliza para el cifrado. No se pasa la clave de cifrado a través de la conexión. Consulte "Modify" en la página 217 para obtener información acerca de la definición de los valores del puerto y de TCP.

Nota: El vector de autenticación se pasará por alto si el direccionador no está protegido con contraseña.

Protocolo de control de antememoria externa

El Protocolo de control de antememoria externa (ECCP) proporciona a los servidores de fondo la capacidad de controlar la antememoria del direccionador. Este control maximiza el rendimiento de la antememoria.

El ECCP es una interfaz de protocolo de arquitectura que permite a los servidores añadir y suprimir objetos, así como modificar las políticas de antememoria.

El gestor de control de antememoria externa se define en el direccionador (Antememoria de Web Server o de Host On-Demand Client) para aceptar conexiones y procesar mandatos destinados a una partición de antememoria.

Configuración

El gestor de control de antememoria externa se configura con los parámetros siguientes:

Puerto definido por el usuario: El número de puerto donde el gestor de control de antememoria externa escucha y acepta conexiones. Si se configura con el valor 0, se supone que el gestor de antememoria externa está inhabilitado.

Valores válidos: de 0 a 65535

Valor por omisión: 0

Valor de tiempo de espera máximo de TCP:

Valores válidos: de 5 a 240 segundos

Valor por omisión: 120

Clave de cifrado: La Clave de cifrado se utilizará si el recuadro está protegido con contraseña. La Clave de cifrado debe componerse de 16 caracteres hexadecimales (0-9, a-f, A-F).

Descripción de las funciones del gestor de control de antememoria externa

En esta sección se describen las funciones del Gestor de control de antememoria externa.

Adición de un objeto

Puede añadirse un objeto de respuesta HTTP a la partición de antememoria. El formato de los datos del objeto debe ser igual que una respuesta HTTP. El Gestor de control de antememoria externa analizará las cabeceras de la respuesta y extraerá la información necesaria. A continuación, el objeto se añadirá a la antememoria.

La diferencia entre Add Object y Add (Force) Object es que Add (Force) Object pasa por alto las cabeceras Cache_Control que especifican DO o DONT. Todas las demás cabeceras utilizadas por el Proxy HTTP para determinar si se debe colocar un objeto en la antememoria se seguirán utilizando. Para Add Object y Add (Force) Object, el objeto se sustituirá en la partición de la antememoria, sea cual sea su fecha.

Supresión de un objeto

Es posible suprimir un objeto HTTP de la antememoria. Debe proporcionarse el URL del objeto.

Utilización de la tabla de dependencias

Para invalidar objetos, es posible modificar, listar y utilizar la tabla de dependencias de una partición de antememoria.

Al modificar la tabla de dependencias (al añadir o eliminar dependencias), debe proporcionarse la dependencia y el URL de dependencia. Además, hay otras dos maneras de modificar la tabla de dependencias. Una de ellas consiste en restablecer toda la tabla, una dependencia entera (es decir, eliminar por completo la dependencia) o una dependencia de URL (o sea, eliminar la dependencia de URL de todas las dependencias). La otra consiste en realizar una recogida de basura en la tabla de dependencias. La recogida de basura limpia todos los URL de dependencia de la tabla de dependencias que no tengan un objeto con ese mismo URL en la antememoria.

Hay diversas maneras de listar la información incluida en la tabla de dependencias. Puede recuperarse la tabla entera, todos los URL de dependencia de una dependencia específica, o todas las dependencias que tengan un URL de dependencia determinado.

Es posible eliminar (invalidar) los objetos de la antememoria mediante la tabla de dependencias. La tabla de dependencias se comprueba utilizando la dependencia. Cualquier URL de dependencia que exista para esa dependencia se eliminará de la partición de la antememoria.

Inhabilitación/Habilitación de una partición

Esta función permite modificar el estado de la partición de la antememoria. Para utilizar el Gestor de control de antememoria externa, la partición de la antememoria debe estar en el estado correcto. Es preciso inhabilitar la partición de la antememoria para depurar todos los objetos de ella.

Utilización de políticas

Las políticas de una partición se pueden listar o modificar. Cada política puede ejecutarse de forma separada o como parte de un grupo. Al modificar una política, es preciso pasar el tipo correcto de datos para ella. Consulte "Formatos de vector del Protocolo de control de antememoria externa (ECCP)" en la página 183 (Subvector de mandato de política y subvector de respuesta de política) para el formato de datos basado en la política.

Depuración de la partición

Esta función permite que se eliminen todos los objetos que haya en la partición de la antememoria. La partición de la antememoria debe estar en estado inhabilitado para poder depurarla.

Consulta de un objeto

Esta función proporciona la capacidad de comprobar si un objeto se encuentra en la partición de la antememoria. Además, si el objeto está en la partición de la antememoria y tiene la fecha de su última modificación, se devuelve esta fecha. Consulte “Formatos de vector del Protocolo de control de antememoria externa (ECCP)” (Subvector de respuesta de consulta) respecto al formato de la fecha devuelta.

Utilización de estadísticas

Esta función proporciona la capacidad de listar y restablecer (borrar) las estadísticas de la partición de la antememoria. Consulte “Formatos de vector del Protocolo de control de antememoria externa (ECCP)” (Subvector de respuesta de estadísticas) respecto al formato de las estadísticas.

Utilización de una máscara de URL

Esta función proporciona la capacidad de listar y modificar las máscaras de URL para una partición de la antememoria. Al utilizar esta función, es preciso proporcionar el tipo de URL de inclusión, exclusión, dinámica o applet de Antememoria de Host On-Demand Client. Debe listar un solo tipo de URL. Esta función no funciona con varios tipos de URL.

El usuario tiene la capacidad de añadir una máscara de URL. Si la máscara de URL es una máscara de inclusión, dinámica, o de applet de Antememoria de Host On-Demand Client, es necesario proporcionar la duración. La adición de una máscara dinámica modificará la máscara de URL dinámica actual, mientras que la adición de una máscara de applet de Antememoria de Host On-Demand Client modificará la máscara actual de applet de Antememoria de Host On-Demand Client. El usuario tiene la capacidad de suprimir una máscara de URL. Esta función no es válida para la máscara de URL dinámica ni para la máscara de applet de Antememoria de Host On-Demand Client. El usuario tiene la capacidad de restablecer todas las máscaras de URL de un tipo determinado. Al restablecer la máscara de URL dinámica, lo hace a la máscara de URL dinámica por omisión, mientras que al restablecer la máscara de applet de Antememoria de Host On-Demand Client, lo hace a la máscara de applet de Antememoria de Host On-Demand Client por omisión.

Nota: La máscara dinámica se utiliza con imágenes de Antememoria de Web Server, mientras que la máscara de applet de Antememoria de Host On-Demand Client se utiliza con imágenes que tienen la característica Antememoria de Host On-Demand Client.

Formatos de vector del Protocolo de control de antememoria externa (ECCP)

Los clientes de ECCP envían mandatos y reciben respuestas mediante un formato de vector. El vector de autenticación es necesario si el recuadro está protegido con contraseña. Si el recuadro no está protegido, se pasa por alto el vector de autenticación cuando se recibe.

Formatos de vector

En esta sección se describen las descripciones de campo para los vectores.

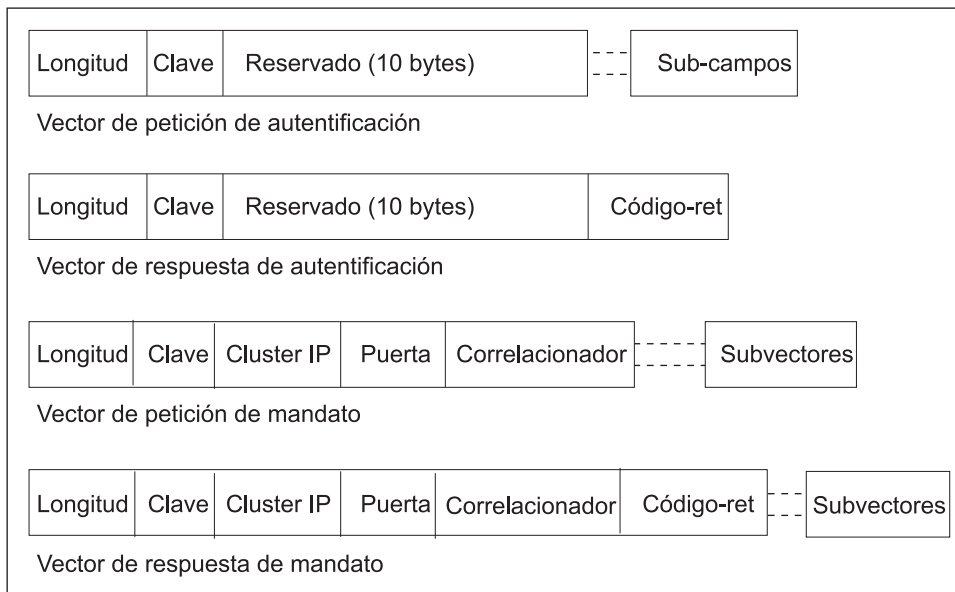


Figura 17. Vector de respuesta de mandato

Longitud: valor de 32 bits sin signo, que representa la longitud (en bytes) del vector completo, incluidos los campos de longitud y de clave, así como los subvectores y subcampos. El rango aceptable es de 22-4 GB para los vectores de mandato y 38-52 para los vectores de autenticación.

Clave: valor de 16 bits sin signo que representa la clave de vector principal. Las claves de vector principales son:

- 0x4A00 (Vector de petición de autenticación)
- 0x4A01 (Vector de respuesta de autenticación)
- 0x4B00 (Vector de petición de mandato)
- 0x4B01 (Vector de respuesta de mandato)

IP cluster: Dirección IP del cluster de antememoria asociado a la partición de antememoria de destino.

Puerto: Número de puerto del cluster de antememoria asociado a la partición de antememoria.

Correlacionador: valor de 32 bits sin signo utilizado por el cliente ECCP para asociar la respuesta de mandato a la petición de mandato.

Códigoret: valor de 32 bits sin signo que representa el código de retorno. Sólo existe en los vectores de respuesta.

Los vectores contienen uno o más subvectores. El vector de petición de autenticación requiere los subcampos de nombre y contraseña. El vector de petición de mandato contiene uno o más subvectores de mandato. Si hay varios subvectores en el vector de petición de mandato, habrá varios subvectores en el vector de res-

puesta de mandato. Si se produce un error grave, queda reflejado en el campo Códigoret del vector de respuesta de mandato.

Vector de petición de autenticación

El Vector de petición de autenticación debe ser el primer vector de la Conexión de control de antememoria externa si el recuadro está protegido con contraseña. Si el recuadro no está protegido con contraseña, se pasa por alto este vector.

- 0-3** Longitud
Longitud (en bytes) del vector, incluidos los campos de longitud y clave, así como los subvectores que haya.
- 4-5** Clave
0x4A00
- 6-15** Reservado
Reservado para su uso en el futuro.
- 16-n** Subcampo de nombre.
- n+1-m** Subcampo de contraseña

Vector de petición de mandato

El Vector de petición de mandato envía mandatos al Gestor de control de antememoria externa. Si el recuadro está protegido con contraseña, el Gestor de control de antememoria externa debe recibir en primer lugar un Vector de petición de autenticación válido, antes de que se acepten los mandatos.

- 0-3** Longitud
Longitud (en bytes) del vector, incluidos los campos de longitud y clave, así como los subvectores que haya.
- 4-5** Clave
0x4B00
- 6-9** Dirección IP de cluster
Dirección IP de un cluster de antememoria (Proxy HTTP) asociada a la partición de antememoria de destino.
- 10-11** Puerto
Número de puerto del cluster de antememoria (Proxy HTTP) asociado a la partición de antememoria de destino.
- 12-15** Correlacionador
El correlacionador se utiliza para asociar las respuestas de mandato a su petición de mandato correspondiente.
- 16-n** Subvectores
Puede añadirse uno o más de los subvectores siguientes.
- Subvector de mandato Add Object (0x0100)
 - Subvector de mandato Add (Force) Object (0x0110)
 - Subvector de mandato Delete Object (0x0400)
 - Subvector de mandato Dependency (0x0A00)

Utilización de la Antememoria del servidor de la web

- Subvector de mandato Disable (0x0300)
- Subvector de mandato Enable (0x0200)
- Subvector de mandato Policy (0x0500)
- Subvector de mandato Purge (0x0600)
- Subvector de mandato Query (0x0700)
- Subvector de mandato Statistics (0x0800)
- Subvector de mandato URL Mask (0x900)

Vector de respuesta de autenticación

Se devuelve el Vector de respuesta de autenticación en respuesta a un Vector de petición de autenticación.

0-3	Longitud	Longitud (en bytes) del vector, incluidos los campos de longitud y clave, así como los subvectores que haya.
4-5	Clave	0x4A01
6-15	Reservado	Reservado para su uso en el futuro.
16-19	Código de retorno	Es el código de retorno para el vector. Vea “Códigos de retorno” en la página 204.
20-n	Subvectores	Actualmente no hay ningún vector en el Vector de respuesta de autenticación.

Vector de respuesta de mandato

Se devuelve el Vector de respuesta de mandato en respuesta a un Vector de petición de mandato.

0-3	Longitud	Longitud (en bytes) del vector, incluidos los campos de longitud y clave, así como los subvectores que haya.
4-5	Clave	0x4B01
6-9	Dirección IP de cluster	Dirección IP de cluster de un cluster de antememoria (Proxy HTTP) asociado a la partición de antememoria de destino.
10-11	Puerto	Número de puerto del cluster de antememoria (Proxy HTTP) asociado a la partición de antememoria de destino.
12-15	Correlacionador	El correlacionador se utiliza para asociar las respuestas de mandato a su petición de mandato correspondiente.

16-19 Código de retorno

Es el código de retorno para el vector. Vea “Códigos de retorno” en la página 204.

20-n Subvectores

Se pueden añadir los subvectores siguientes, o no añadir ninguno.

- Subvector de respuesta a Add Object (0x0101)
- Subvector de respuesta a Add (Force) Object (0x0111)
- Subvector de respuesta a Delete Object (0x0401)
- Subvector de respuesta a Dependency (0x0A01)
- Subvector de respuesta a Disable (0x0301)
- Subvector de respuesta a Enable (0x0201)
- Subvector de respuesta a Policy (0x0501)
- Subvector de respuesta a Purge (0x0601)
- Subvector de respuesta a Query (0x0701)
- Subvector de respuesta a Statistics (0x0801)
- Subvector de respuesta a URL Mask (0x901)

Formatos de subvector

En esta sección se describen los formatos de subvector. Los subvectores siguen el mismo formato básico que el vector principal:

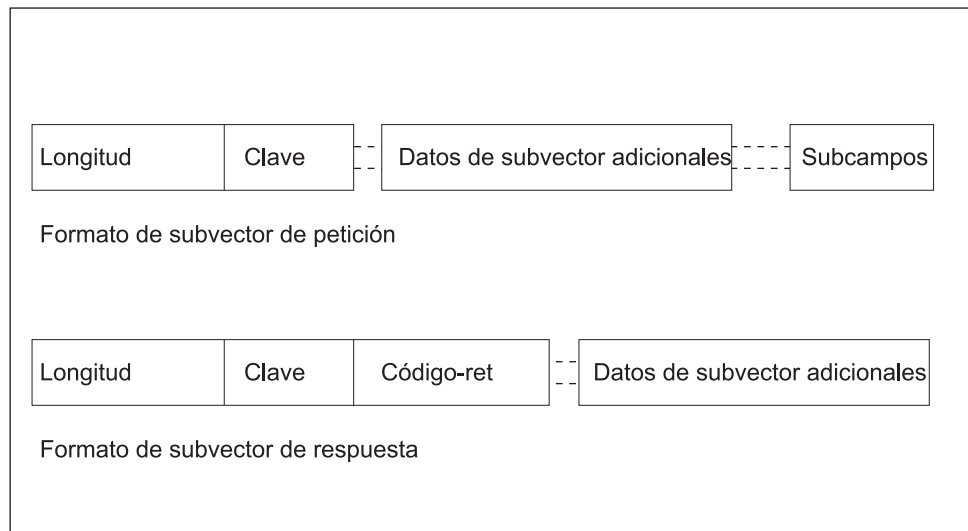


Figura 18. Formato de subvector

Longitud: valor de 32 bits sin signo, que representa la longitud (en bytes) del subvector completo, incluidos los campos de longitud y de clave, así como los subcampos. El rango aceptable es de 6-4 GB (no se comprueba el límite superior)

Clave: valor de 16 bits sin signo que representa la clave de subvector. Las claves de subvector de petición son:

- 0x0100 (Añadir objeto WEB)

Utilización de la Antememoria del servidor de la web

- 0x0110 (Añadir objeto WEB, pasar por alto las cabeceras de control de antememoria)
- 0x0200 (Habilitar la colocación en antememoria en la partición)
- 0x0300 (Inhabilitar la colocación en antememoria en la partición)
- 0x0400 (Suprimir un objeto WEB)
- 0x0500 (Modificar o listar políticas de antememoria)
- 0x0600 (Eliminar todos los objetos WEB de la partición)
- 0x0700 (Determinar si hay un objeto WEB en la partición)
- 0x0800 (Restablecer o listar las estadísticas de la antememoria)
- 0x0900 (Añadir, suprimir, listar máscaras de URL)
- 0x0A00 (Añadir, suprimir, listar, restablecer dependencias)

Las claves de subvector de respuesta que se devuelven son:

- 0x0101 (Añadir objeto WEB)
- 0x0111 (Añadir objeto WEB, pasar por alto las cabeceras de control de antememoria)
- 0x0201 (Habilitar la colocación en antememoria en la partición)
- 0x0301 (Inhabilitar la colocación en antememoria en la partición)
- 0x0401 (Suprimir un objeto WEB)
- 0x0501 (Modificar o listar políticas de antememoria)
- 0x0601 (Eliminar todos los objetos WEB de la partición)
- 0x0701 (Determinar si hay un objeto WEB en la partición)
- 0x0801 (Restablecer o listar las estadísticas de la antememoria)
- 0x0901 (Añadir, suprimir, listar máscaras de URL)
- 0x0A01 (Añadir, suprimir, listar, restablecer dependencias)

Códigoret: valor de 32 bits sin signo que representa el código de retorno para el subvector de petición. Sólo existe en el subvector de respuesta.

Subvector de mandato Add Object: El Subvector de mandato Add Object se utiliza para añadir un Objeto Web a la partición de la antememoria.

0-3	Longitud
	Longitud (en bytes) del vector, incluidos los campos de longitud y clave, así como los subvectores que haya.
4-5	Clave
	0x0110
6-n	Subcampo URL
n+1-m	Subcampo Object

Subvector de mandato Add (force) Object: El Subvector de mandato Add (force) Object se utiliza para añadir un Objeto Web a la partición de la antememoria. Difiere del Subvector de mandato Add Object en que se pasan por alto las cabeceras de Control de antememoria del objeto.

- 0-3** Longitud
 Longitud (en bytes) del vector, incluidos los campos de longitud y clave, así como los subvectores que haya.
- 4-5** Clave
 0x0100
- 6-n** Subcampo URL
- n+1-m** Subcampo Object

Subvector de mandato Delete Object: El Subvector de mandato Delete Object se utiliza para eliminar un Objeto Web de la partición de la antememoria.

- 0-3** Longitud
 Longitud (en bytes) del vector, incluidos los campos de longitud y clave, así como los subvectores que haya.
- 4-5** Clave
 0x0400
- 6-n** Subcampo URL

Subvector de mandato Dependency: El Subvector de mandato Dependency se utiliza para modificar/listar la Tabla de dependencias o invalidar objetos mediante la Tabla de dependencias.

- 0-3** Longitud
 Longitud (en bytes) del vector, incluidos los campos de longitud y clave, así como los subvectores que haya.
 - 4-5** Clave
 0x0A00
 - 6-7** Mandato
 El mandato Dependency que se va a ejecutar.
- 0x0001** Obtener la tabla de dependencias (vea la dependencia en Tipo de dependencia)
 - 0x0002** Añadir una nueva dependencia/URL de dependencia a la Tabla de dependencias
 - 0x0003** Eliminar una dependencia/URL de dependencia de la Tabla de dependencia
 - 0x0004** Restablecer la información de la tabla de dependencias (vea la dependencia en Tipo de dependencia)
 - 0x0005** Invalidar un objeto basado en una dependencia
 - 0x0006** Recogida de basura de la Tabla de dependencias

8-9 Tipo de dependencia

El campo de tipo de dependencia se utiliza para identificar los datos que se van a modificar. Entonces, estos datos se modifican utilizando el mandato Dependency.

0x0000 Ningún tipo de dependencia

0x0001 Utilizar el mandato en toda la tabla.

- Si el mandato anterior es 0x0001 (Get) - obtener la tabla entera.
- Si el mandato anterior es 0x0004 (Reset) - borrar la tabla entera.

0x0002 Utilizar el mandato basándose en la dependencia.

- Si el mandato anterior es 0x0001 (Get) - obtener todos los URL para la dependencia dada.
- Si el mandato anterior es 0x0004 (Reset) - borrar una dependencia de la tabla.

0x0003 Utilizar el mandato basándose en el URL

- Si el mandato anterior es 0x0001 (Get) - obtener toda la dependencia para el URL de dependencia dado.
- Si el mandato anterior es 0x0004 (Reset) - borrar un URL de dependencia de la tabla.

10-n Cero o más subcampos.

Subcampo Dependency

Nota: Este subcampo debe ser el primero cuando ambos subcampos son obligatorios.

Obligatorio cuando se tiene este mandato-tipo de dependencia.

Mandato	Tipo de dependencia
0x0001	0x0002
0x0002	0x0000
0x0003	0x0000
0x0004	0x0002
0x0005	0x0000

Subcampo URL

Nota: Este subcampo debe ser el segundo cuando ambos subcampos son obligatorios. Obligatorio cuando se tiene este mandato-tipo de dependencia.

Mandato	Tipo de dependencia
0x0001	0x0003
0x0002	0x0000
0x0003	0x0000
0x0004	0x0003

Subvector de mandato Disable: El Subvector de mandato Disable se utiliza para inhabilitar una partición de antememoria.

0-3 Longitud

Longitud (en bytes) del vector, incluidos los campos de longitud y clave, así como los subvectores que haya.

4-5 Clave

0x0300

Subvector de mandato Enable: El Subvector de mandato Enable se utiliza para habilitar una partición de antememoria.

- 0-3** Longitud
Longitud (en bytes) del vector, incluidos los campos de longitud y clave, así como los subvectores que haya.
- 4-5** Clave
0x0200

Subvector de mandato Policy: El Subvector de mandato Policy permite modificar una partición de antememoria o listar la información en una partición de antememoria.

- 0-3** Longitud
Longitud (en bytes) del vector, incluidos los campos de longitud y clave, así como los subvectores que haya.
- 4-5** Clave
0x0500
- 6-7** Mandato
El mandato que se va a ejecutar.
0x0001 Obtener una política
0x0002 Actualizar una política
- 8-9** Tipo de política
El Tipo de política se utiliza para identificar los datos que se van a modificar. Entonces, estos datos se modifican utilizando el mandato Policy.
0x0001 Colocación en antememoria transparente
0x0002 Cabecera de control de antememoria HTTP
0x0003 Colocar en antememoria los objetos dinámicos
0x0004 Colocar en antememoria los objetos de imagen (*.gif, *.jpg)
0x0005 Colocar en antememoria los objetos estáticos
0x0006 Duración por omisión de los objetos dinámicos
0x0007 Duración por omisión de los objetos de imagen
0x0008 Duración por omisión de los objetos estáticos.
0x0009 Tiempo (en segundos) entre las recogidas de basura.
0x000A Tamaño máximo de partición (en MB).
0x000B Número máximo de objetos en una partición de antememoria.
0x000C Tamaño máximo del objeto en una partición de antememoria.
0xFFFF Operar en todas las políticas.

Nota: Si el mandato es Get (0x0001), éste es el final del subvector.

Utilización de la Antememoria del servidor de la web

- 10-n** Uno de los siguientes, según el Tipo de política indicado anteriormente.
Si el Tipo de política = 0x0001, 0x0002, 0x0003, 0x0004 ó 0x0005:
- 10-11** Definir valor
- 0x0001 (Habilitado)
 - 0x0002 (Inhabilitado)
- Si el Tipo de política = 0x0006, 0x0007 ó 0x0008
- 10-13** El valor que representa la duración del objeto en minutos.
El rango abarca de 0 a 10080, donde 0 representa un objeto sin caducidad.
- Si el Tipo de política = 0x0009
- 10-13** El valor que representa el intervalo de depuración de antememoria en minutos.
El rango abarca de 0 a 720, donde 0 indica que debe inhabilitarse la recogida de basura.
- Si el Tipo de política = 0x000A
- 10-11** Un valor que representa el tamaño máximo de partición en MB. El rango es 0-4095, donde 0 indica que no hay límite.
Nota: No se verifica el valor.
- Si la Política = 0x000B
- 10-13** Un valor que representa el número máximo de objetos.
El rango es 0-100000, donde 0 indica que no hay límite.
Nota: No se verifica el valor.
- Si la Política = 0x000C
- 10-13** Un valor que representa el tamaño máximo de un objeto en la partición de antememoria.
El rango es de 512 a 300000, donde entrar 0 indica que no hay límite.
Nota: No se verifica el valor.
- Si la Política = 0xFFFF
- 10-11** Colocación transparente en antememoria (Definir valor)
- 0x0001 (Habilitado)
 - 0x0002 (Inhabilitado)
- 12-13** Cabecera de control de antememoria HTTP (Definir valor)
- 0x0001 (Habilitado)
 - 0x0002 (Inhabilitado)
- 14-15** Colocación dinámica en antememoria (Definir valor)
- 0x0001 (Habilitado)
 - 0x0002 (Inhabilitado)

- 16-17** Colocación de imagen en antememoria (Definir valor)
- 0x0001 (Habilitado)
 - 0x0002 (Inhabilitado)
- 18-19** Colocación estática en antememoria (Definir valor)
- 0x0001 (Habilitado)
 - 0x0002 (Inhabilitado)
- 20-21** Un valor que representa el tamaño máximo de partición en MB.
- El rango abarca de 0 a 4095, donde 0 indica que no hay límite.
- Nota:** No se verifica el valor.
- 20-21** Un valor que representa el tamaño máximo de partición en MB.
- El rango abarca de 0 a 4095, donde 0 indica que no hay límite.
- Nota:** No se verifica el valor.
- 22-25** Un valor que representa el número máximo de objetos.
- El rango abarca de 0 a 1000000, donde 0 indica que no hay límite.
- Nota:** No se verifica el valor.
- 26-29** Un valor que representa el tamaño máximo de un objeto en una partición de antememoria.
- El rango abarca de 512 a 3000000, donde especificar 0 indica que no hay límite.
- Nota:** No se verifica el valor.
- 30-33** El valor que representa la duración del objeto dinámico en minutos.
- El rango abarca de 0 a 10080, donde 0 representa un objeto sin caducidad.
- Nota:** No se verifica el valor.
- 34-37** El valor que representa la duración del objeto de imagen en minutos.
- El rango abarca de 0 a 10080, donde especificar 0 indica que no hay límite.
- Nota:** No se verifica el valor.
- 38-41** El valor que representa la duración del objeto estático en minutos.
- El rango abarca de 0 a 10080, donde 0 representa que no hay límite.
- Nota:** No se verifica el valor.

- 42-45** El valor que representa el intervalo de depuración de antememoria en minutos.
El rango abarca de 0 a 720, donde 0 indica que debe habilitarse la recogida de basura.

Subvector de mandato Purge: El Subvector de mandato Purge se utiliza para borrar todos los objetos de una partición de antememoria.

- 0-3** Longitud
Longitud (en bytes) del vector, incluidos los campos de longitud y clave, así como los subvectores que haya.
- 4-5** Clave
0x0600

Subvector de mandato Query: El Subvector de mandato Query se utiliza para comprobar si hay un URL determinado en la partición de la antememoria.

- 0-3** Longitud
Longitud (en bytes) del vector, incluidos los campos de longitud y clave, así como los subvectores que haya.
- 4-5** Clave
0x0700
- 6-n** Subcampo URL

Subvector de mandato Statistics: El Subvector de mandato Statistics se utiliza para obtener/restablecer las estadísticas de una partición de antememoria.

- 0-3** Longitud
Longitud (en bytes) del vector, incluidos los campos de longitud y clave, así como los subvectores que haya.
- 4-5** Clave
0x0800
- 6-7** Mandato
- 0x0001 - Obtener las estadísticas para la partición de la antememoria.
 - 0x0004 - Restablecer las estadísticas para la partición de la antememoria.

Subvector de mandato URL Mask: El Subvector de mandato URL Mask se utiliza para listar/modificar las máscaras de URL asociadas a una partición de antememoria.

- 0-3** Longitud
Longitud (en bytes) del vector, incluidos los campos de longitud y clave, así como los subvectores que haya.
- 4-5** Clave
0x0900

6-7 Mandato

- 0x0001 - Obtener las máscaras URL definidas actualmente (consulte el Tipo de URL más abajo para ver el tipo de máscaras que se devolverá).
- 0x0002 - Añadir la máscara de URL determinada (consulte el Tipo de URL más abajo para ver el tipo de máscara que se añadirá).
- 0x0003 - Suprimir la máscara de URL determinada (consulte el Tipo de URL más abajo para el tipo de máscara que se suprimirá).

Nota: La supresión de la máscara de URL dinámica o la máscara de la applet Antememoria de Host-On-Demand Client es una función no válida.

- 0x0004 - Restablecer toda la máscara de URL del Tipo de URL dado más abajo.

8-9 El tipo de URL

- 0x0001 - Inclusión
- 0x0002 - Exclusión
- 0x0003 - Dinámico
- 0x0004 - Applet de Antememoria de Host On-Demand Client

10-13 Duración

El rango abarca de 0 a 10080, donde 0 representa un objeto sin caducidad. Se utiliza sólo para el mandato Add (0x0002) cuando el Tipo de URL es Inclusión (0x0001), Dinámico (0x0003) o applet de Antememoria de Host On-Demand Client (0x0004).

Nota: Si el mandato es GET (0x0001) o Clear (0x0004), éste es el final del subvector.

14-n Un subvector de mandato URL.

Subvector de respuesta a Add Object: El Subvector de respuesta a Add Object se utiliza para responder a un subvector de mandato Add (Force) Object.

0-3 Longitud

Longitud (en bytes) del vector, incluidos los campos de longitud y clave, así como los subvectores que haya.

4-5 Clave

0x0101

6-9 Código de retorno

Vea "Códigos de retorno" en la página 204.

Subvector de respuesta a Add (Force): El Subvector de respuesta a Add (Force) se utiliza para responder a un subvector de mandato Add (Force) Object.

0-3 Longitud

Longitud (en bytes) del vector, incluidos los campos de longitud y clave, así como los subvectores que haya.

Utilización de la Antememoria del servidor de la web

- 4-5 Clave
0x0111
- 6-9 Código de retorno

Vea “Códigos de retorno” en la página 204.

Subvector de respuesta a Delete Object: El Subvector de respuesta a Delete Object se utiliza para responder a un subvector de mandato Add (Force) Object.

- 0-3 Longitud
Longitud (en bytes) del vector, incluidos los campos de longitud y clave, así como los subvectores que haya.
- 4-5 Clave
0x0401
- 6-9 Código de retorno
Vea “Códigos de retorno” en la página 204.

Subvector de respuesta a Dependency: El Subvector de respuesta a Dependency se utiliza para responder a un Subvector de mandato Dependency.

- 0-3 Longitud
Longitud (en bytes) del vector, incluidos los campos de longitud y clave, así como los subvectores que haya.
- 4-5 Clave
0x0A01
- 6-9 Código de retorno
Vea “Códigos de retorno” en la página 204.
- 10-n Cero o más subcampos.
- Subcampo Dependency**
Nota: Este subcampo debe incluirse antes que los subcampos del mandato URL dirigidos a la dependencia. Es obligatorio cuando se tiene este mandato-tipo de dependencia.
Para obtener más información, consulte “Subvector de mandato Dependency” en la página 189.

Mandato	Tipo de dependencia	
0x0001	0x0001	Nota: cualquier subcampo de URL que sigue al subcampo Dependency son los URL de dependencia para esa dependencia.
0x0001	0x0003	

Subcampo URL
Nota: Este subcampo debe ser el segundo cuando ambos subcampos son obligatorios. Obligatorio cuando se tiene este mandato-tipo de dependencia.

Mandato	Tipo de dependencia	
0x0001	0x0001	Nota: el subcampo Dependency anterior al subcampo URL indica el URL para la dependencia.
0x0001	0x0002	

Subvector de respuesta a Disable: El Subvector de respuesta a Disable se utiliza para responder al Subvector de mandato Disable.

- 0-3** Longitud
Longitud (en bytes) del vector, incluidos los campos de longitud y clave, así como los subvectores que haya.
- 4-5** Clave
0x0301
- 6-9** Código de retorno
Vea “Códigos de retorno” en la página 204.

Subvector de respuesta a Enable: El Subvector de respuesta a Enable se utiliza para responder al Subvector de mandato Enable.

- 0-3** Longitud
Longitud (en bytes) del vector, incluidos los campos de longitud y clave, así como los subvectores que haya.
- 4-5** Clave
0x0201
- 6-9** Código de retorno
Vea “Códigos de retorno” en la página 204.

Subvector de respuesta a Policy: El Subvector de respuesta a Policy se utiliza para responder al Subvector de mandato Policy.

- 0-3** Longitud
Longitud (en bytes) del vector, incluidos los campos de longitud y clave, así como los subvectores que haya.
- 4-5** Clave
0x0501
- 6-9** Código de retorno
Vea “Códigos de retorno” en la página 204.

Si el Subvector de mandato Policy era PUT (0x0002), es el final del subvector.

- 10-n** Uno de los siguientes, según el Tipo de política del Subvector de mandato Policy.
Si el Tipo de política = 0x0001, 0x0002, 0x0003, 0x0004 ó 0x0005:
- 10-11** Definir valor
- 0x0001 (Habilitado)
 - 0x0002 (Inhabilitado)
- Si el Tipo de política = 0x0006, 0x0007 ó 0x0008
- 10-13** El valor que representa la duración del objeto en minutos.
El rango abarca de 0 a 10080, donde 0 representa un objeto sin caducidad.
- Si el Tipo de política = 0x0009

Utilización de la Antememoria del servidor de la web

- 10-13** El valor que representa el intervalo de depuración de antememoria en minutos.
El rango abarca de 0 a 720, donde 0 indica que debe inhabilitarse la recogida de basura.

Si el Tipo de política = 0x000A

- 10-11** Un valor que representa el tamaño máximo de partición en MB. El rango es 0-4095, donde 0 indica que no hay límite.
Nota: No se verifica el valor.

Si la Política = 0x000B

- 10-13** Un valor que representa el número máximo de objetos.
El rango es 0-100000, donde 0 indica que no hay límite.
Nota: No se verifica el valor.

Si la Política = 0x000C

- 10-13** Un valor que representa el tamaño máximo de un objeto en la partición de antememoria.
El rango es de 512 a 300000, donde entrar 0 indica que no hay límite.
Nota: No se verifica el valor.

Si la Política = 0xFFFF

- 10-11** Colocación transparente en antememoria (Definir valor)
- 0x0001 (Habilitado)
 - 0x0002 (Inhabilitado)

- 12-13** Cabecera de control de cabecera HTTP (Definir valor)
- 0x0001 (Habilitado)
 - 0x0002 (Inhabilitado)

- 14-15** Colocación dinámica en antememoria (Definir valor)
- 0x0001 (Habilitado)
 - 0x0002 (Inhabilitado)

- 16-17** Colocación de imagen en antememoria (Definir valor)
- 0x0001 (Habilitado)
 - 0x0002 (Inhabilitado)

- 18-19** Colocación estática en antememoria (Definir valor)
- 0x0001 (Habilitado)
 - 0x0002 (Inhabilitado)

- 20-21** Un valor que representa el tamaño máximo de partición en MB.
El rango abarca de 0 a 4095, donde 0 indica que no hay límite.
Nota: No se verifica el valor.

- 22-25** Un valor que representa el número máximo de objetos.
El rango abarca de 0 a 1000000, donde 0 indica que no hay límite.
Nota: No se verifica el valor.
- 26-29** Un valor que representa el tamaño máximo de un objeto en una partición de antememoria.
El rango abarca de 512 a 3000000, donde especificar 0 indica que no hay límite.
Nota: No se verifica el valor.
- 30-33** El valor que representa la duración del objeto dinámico en minutos.
El rango abarca de 0 a 10080, donde 0 representa un objeto sin caducidad.
Nota: No se verifica el valor.
- 34-37** El valor que representa la duración del objeto de imagen en minutos.
El rango abarca de 0 a 10080, donde especificar 0 indica que no hay límite.
Nota: No se verifica el valor.
- 38-41** El valor que representa la duración del objeto estático en minutos.
El rango abarca de 0 a 10080, donde 0 representa que no hay límite.
Nota: No se verifica el valor.
- 42-45** El valor que representa el intervalo de depuración de antememoria en minutos.
El rango abarca de 0 a 720, donde 0 indica que debe inhabilitarse la recogida de basura.

Subvector de respuesta a Purge: El Subvector de respuesta a Purge se utiliza para responder a un Subvector de mandato Purge.

- 0-3** Longitud
Longitud (en bytes) del vector, incluidos los campos de longitud y clave, así como los subvectores que haya.
- 4-5** Clave
0x0601
- 6-9** Vea “Códigos de retorno” en la página 204.

Subvector de respuesta a Query: El Subvector de respuesta a Query se utiliza para comprobar si hay un URL determinado en la partición de la antememoria.

- 0-3** Longitud
Longitud (en bytes) del vector, incluidos los campos de longitud y clave, así como los subvectores que haya.

Utilización de la Antememoria del servidor de la web

- 4-5** Clave
0x0701
- 6-9** Código de retorno
Vea “Códigos de retorno” en la página 204.
- Nota:** Si el código de retorno indica una anomalía (no es 0x00000000), éste es el final de la respuesta.
- 10-37** La hora en que se ha modificado el objeto por última vez, en el huso horario GMT.
- Nota:** Este campo no existirá si el código de retorno no era 0x00000000, o si la Partición de antememoria no lo conoce.
- 10-13** Segundos
- 14-17** Minutos
- 18-21** Horas
- 22-25** Meses desde enero (0-11)
- 26-29** Años desde 1900
- 30-33** Días desde el domingo (0-6)
- 34-37** Día del mes

Subvector de respuesta a Statistics: El Subvector de respuesta a Statistics responde al Subvector de mandato Statistics.

- 0-3** Longitud
Longitud entera (en bytes) del vector, incluidos los campos de longitud y clave, así como los subvectores que haya.
- 4-5** Clave
0x0801
- 6-9** Código de retorno
Es el código de retorno para el subvector.
- 10-**
- 10-13** Número actual de bytes en la Partición de antememoria. El número sólo refleja los bytes de entidad y no incluye los bytes utilizados para almacenar las cabeceras o la utilización de bloques de control.
- 14-17** Marca de nivel para el número de bytes en la Partición de antememoria.
- 18-21** Número actual de objetos en la Partición de antememoria.
- 22-25** Marca de nivel para el número de objetos en la Partición de antememoria.
- 26-29** Número total de veces que se han encontrado objetos en la Partición de antememoria.
- 30-33** Número total de veces que no se han encontrado objetos en la Partición de antememoria.

- 34-37** Número de objetos añadidos explícitamente a la Partición de antememoria por la máscara de URL de Inclusión.
- 40-43** Número de objetos no añadidos a la Partición de antememoria, porque se ha desactivado la colocación en antememoria.
- 44-47** Número de objetos no añadidos a la partición de antememoria, porque el objeto es demasiado grande.
- 48-51** Número de objetos no añadidos a la Partición de antememoria, porque se ha especificado DONT CACHE en la cabecera de control HTTP.
- 52-55** Número de objetos no añadidos a la Partición de antememoria, porque la máscara de URL los ha excluido explícitamente.
- 56-59** Número de objetos no añadidos a la Partición de antememoria, porque el objeto es sobrante.
- 60-63** Número de objetos no añadidos a la Partición de antememoria, porque el objeto de imagen no se coloca explícitamente en antememoria.
- 64-67** Número de objetos no añadidos a la Partición de antememoria, porque el objeto estático no se coloca explícitamente en antememoria.
- 68-71** Número de objetos no añadidos a la Partición de antememoria, porque el objeto dinámico no se coloca explícitamente en antememoria.
- 72-75** Número de objetos depurados, debido a que la antememoria está llena o todas las particiones de antememoria exceden la cantidad total permitida por la Antememoria del servidor de la web.
- 76-79** Número de objetos depurados debido a la caducidad de la duración de los objetos.
- 80-83** Número de objetos depurados explícitamente, proporcionando el URL o depurando toda la partición.
- 84-87** Número de objetos depurados debido a que la dependencia no es válida.

Subvector de respuesta a URL Mask: El Subvector de respuesta a URL Mask se utiliza para responder a un Subvector de mandato URL Mask.

- 0-3** Longitud
Longitud (en bytes) del vector, incluidos los campos de longitud y clave, así como los subvectores que haya.
- 4-5** Clave
0x0901
- 6-9** Código de retorno
Es el código de retorno para el subvector. Vea “Códigos de retorno” en la página 204.

10-n Cero o más Subvectores de URL, si el Subvector de mandato URL Mask era GET (0x0001).

Formatos de subcampo

Esta sección describe las descripciones de campo para los subcampos.

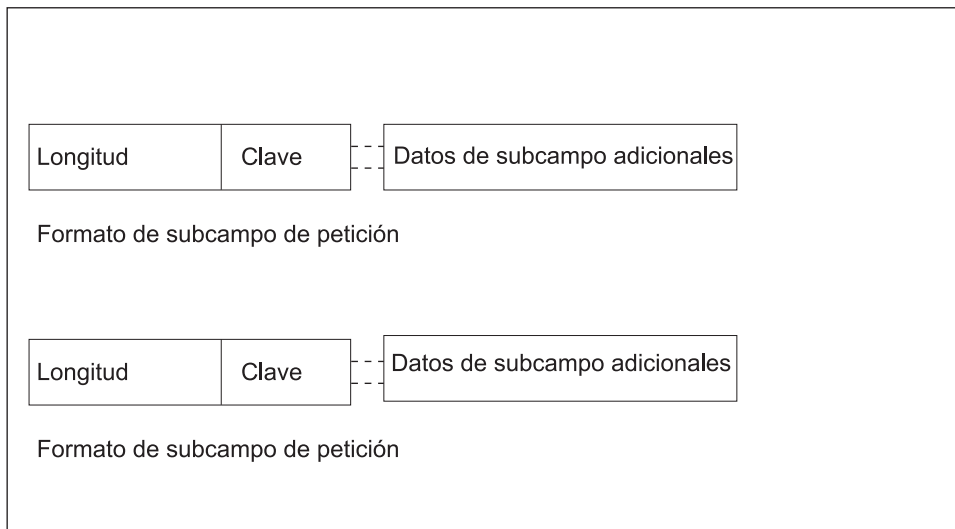


Figura 19. Formato de subcampo

Longitud: valor de 32 bits sin signo, que representa la longitud (en bytes) del subcampo entero, incluidos los campos de longitud y de clave. El rango aceptable es de 6-4 GB.

Clave: valor de 16 bits sin signo que representa la clave de subcampo. Las claves de subcampo de mandato contienen:

- 0x0010 (Localizador uniforme de recursos, separado del protocolo "http:" y la dirección del recurso Internet. Por ejemplo, el URL "http://192.9.200.50/file1.html" se enviará como "/file1.html").
- 0x0020 (Objeto WEB en un formato de mensaje de respuesta HTTP)
- 0x0030 (Nombre de usuario ECCP. Este subcampo es obligatorio para el vector de autenticación).
- 0x0040 (Contraseña de usuario ECCP. Este subcampo es obligatorio para el vector de autenticación).
- 0x0050 (Subcampo Dependency)

Las claves del subcampo de respuesta son:

- 0x0011 (Localizador uniforme de recursos, separado del protocolo "http:" y la dirección del recurso Internet).
- 0x0051 (Subcampo Dependency)

Subcampo Dependency: El subcampo Dependency para el Subvector de respuesta a URL Mask.

0-3 Longitud

Longitud (en bytes) del vector, incluidos los campos de longitud y clave.

4-5 Clave
0x0050 - petición
0x0051 - respuesta

6-n Dependencia
Debe tener una longitud de 1 a 50.

Subcampo Name: El subcampo Name para el Subvector de respuesta a URL Mask.

0-3 Longitud
Longitud (en bytes) del vector, incluidos los campos de longitud y clave.

4-5 Clave
0x00030 - petición

6-n Nombre
Debe tener una longitud de 1 a 8.

Subcampo Object: El subcampo Object para el Subvector de respuesta a URL Mask.

0-3 Longitud
Longitud (en bytes) del vector, incluidos los campos de longitud y clave.

4-5 Clave
0x002 - petición

6-n Objeto
El objeto debe formatearse como una Respuesta HTTP. Es una matriz de caracteres.

Subcampo Password Request: El subcampo Password Request para el Subvector de respuesta a URL Mask.

0-3 Longitud
Longitud (en bytes) del vector, incluidos los campos de longitud y clave.

4-5 Clave
0x0400

6-14 Número generador utilizado en el cifrado (debe ser de 8 bytes).

15-n Contraseña
Debe tener una longitud de 1 a 8 bytes y estar cifrado.

Subcampo URL Request: El subcampo URL Request para la Respuesta a URL Mask.

0-3 Longitud
Longitud (en bytes) del vector, incluidos los campos de longitud y clave.

- 4-5** Clave
0x0010 - petición
0x0011 - respuesta
- 6-n** URL o Máscara de URL
Es una matriz de caracteres, que debe tener una longitud de 1 a 255.

Códigos de retorno

Es importante comprobar los códigos de retorno para cada subvector de respuesta, además del código de retorno en el vector de respuesta. El código de retorno para el vector de respuesta se definirá con un valor distinto de cero si se ha detectado un error grave, en cuyo caso es posible que los subvectores de mandato del vector de mandato tengan el subvector de respuesta correspondiente.

Códigos de retorno y descripciones

- 0000 0000: La operación se ha realizado satisfactoriamente
0001 0000: Objeto no encontrado
0002 0000: La partición de antememoria ya está habilitada.
0003 0000: La partición de antememoria ya está inhabilitada.
0004 0000: La partición de antememoria no está habilitada.
0005 0000: La partición de antememoria no está definida.
0006 0000: Termina la partición de antememoria
0007 0000: El subcampo URL es obligatorio pero no está
0008 0000: El intervalo de depuración indicado no es válido
0009 0000: Valor de definición no soportado
000A 0000: Valor de mandato no soportado
000B 0000: Valor de tipo de política no soportado
000C 0000: Valor de tipo de URL no soportado
000D 0000: Clave de vector no soportada
000E 0000: Clave de subvector no soportada
000F 0000: Imposible analizar las cabeceras del objeto
0010 0000: Imposible obtener almacenamiento
0011 0000: Objeto demasiado grande para añadirlo a la partición
0012 0000: El formato de vector no es válido
0013 0000: El objeto no se puede colocar en antememoria
0014 0000: Se ha detectado un error de análisis de HTTP
0015 0000: El subcampo Object es obligatorio pero no está
0016 0000: El subcampo Dependency no se ha proporcionado o no es válido
0017 0000: Es necesario un Vector de autenticación
0018 0000: No es necesario un Vector de autenticación y se pasa por alto
0019 0000: La dependencia no estaba en la tabla de dependencias
001A 0000: El URL de dependencia no estaba en la tabla de dependencias
001B 0000: Tipo de dependencia no soportado
001C 0000: ID de usuario/contraseña/permiso erróneo para ECC
001D 0000: Tipo de máscara de URL erróneo para carga de imagen en recuadro
FF01 yyyy: El mandato ha fallado. Los 2 últimos bytes contienen información adicional.
0101: El objeto no se ha encontrado.
0102: El objeto no se ha podido colocar en antememoria.
0103: El objeto ya existe en la partición.
0104: Anomalía en inicialización de partición, ya está activo el número máximo de particiones
0105: La partición está activa.

- 0106: La partición no está activa.
- 0107: La partición está en estado pendiente y no puede ejecutar el mandato.
Espere unos segundos y vuelva a intentar el mandato.
- 0108: La partición no está definida.
- 0109: El tipo de URL no está soportado.
- 010A: El puntero de URL no es válido.
- 010B: El número de partición no es válido.
- 010C: El mandato de partición no está soportado.
- 010D: El puntero de partición no es válido.
- 010E: El manejo de partición no hace referencia a una partición activa.
- 010F: El manejo de partición no hace referencia a una partición válida.
- 0110: El puntero de política es obligatorio pero no está.
- 0111: El puntero de estadísticas es obligatorio pero no está.
- 0112: El intervalo de depuración es demasiado grande.
- 0113: La dependencia ya tiene un URL.
- 0FFF: El control de antememoria externo no está disponible.
- FFF9: Imposible adquirir almacenamiento.
- FFFA: Imposible adquirir manejo de partición.
- FFFB: El puntero de SRAM de política es obligatorio pero no está.
- FFFC: El puntero de SRAM de partición es obligatorio pero no está.
- FFFD: Imposible asignar/inicializar intervalo de caducidad de antememoria.
- FFFE: Imposible asignar/inicializar partición de antememoria.
- FFFF: Imposible asignar/inicializar imagen de memoria de antememoria.

Configuración y supervisión de la Antememoria del servidor de la web

Este capítulo describe cómo configurar la característica Antememoria del servidor de la web y utilizar los mandatos de supervisión de la Antememoria del servidor de la web. Contiene:

- “Configuración de la Antememoria del servidor de la web”
- “Acceso al entorno de la Antememoria del servidor de la web” en la página 214
- “Mandatos de la Antememoria del servidor de la web” en la página 214
- “Acceso al entorno de supervisión de la Antememoria del servidor de la web” en la página 221
- “Mandatos de supervisión de la Antememoria del servidor de la web” en la página 221.

Configuración de la Antememoria del servidor de la web

La Función de colocación en antememoria del servidor de la web debe utilizarse con Network Dispatcher. Antes de utilizar la Antememoria del servidor de la web por primera vez, debe:

1. Acceder a Network Dispatcher en talk 6 desde el indicador Config> mediante el mandato **feature ndr**.
2. Habilitar el ejecutor
3. Añadir un cluster
4. Añadir un puerto
5. Añadir uno o más servidores.

Entonces puede utilizar los mandatos de configuración y supervisión para alterar el entorno de la Antememoria del servidor de la web.

Nota: Aunque los cambios en Network Dispatcher efectuados mediante Talk 6 modifican la configuración que se ejecuta actualmente, los cambios de la Antememoria del servidor de la web no la modifican, a menos que se active de manera explícita a través del mandato **activate** en Talk 6, o mediante la característica Webc de Talk 5. La única excepción es que, si el cluster/puerto de un Proxy HTTP se elimina mediante la característica NDR de Talk 6, esto hará que el Proxy HTTP de la Antememoria del servidor de la web se elimine también de la configuración que se ejecuta actualmente.

Ejemplo:

```
Config>f ndr
NDR Config>enable executor
NDR Config>add cluster
Cluster Address [0.0.0.0]? 113.3.1.10
FIN count [4000]?
FIN time out [30]?
FIN stale timer [1500]?
Cluster 113.3.1.12 has been added.
Fincount has been set to 4000 for cluster 113.3.1.10
Fintimeout has been set to 30 for cluster 113.3.1.10
Staletimer has been set to 1500 for cluster 113.3.1.10
NDR Config>add port
Cluster Address [0.0.0.0]? 113.3.1.10
Port number [80]?
Port type (tcp=1, upd=2, both=3) [3]?
Max. weight (0-100) [20]?
Only one pftp port per cluster allowed
Port mode (none=0, sticky=1 pftp=2 cache=3 extcache=4) [0]? 3
Do you want a new cache partition? [Yes]:
Enter cache partition [0]?
Default server TCP connection timeout (Range 5-240 seconds) [120]?
Default client TCP connection timeout (Range 5-240 seconds) [120]?
Maximum partition size (1-4095 megabytes or 0 for no limit) [0]?
Maximum number of objects (1-100000 or 0 for no limit) [0]?
Maximum object size (512-300000 bytes or 0 for no limit) [0]?
Do you want the cache activated upon reboot? [Yes]:
Default cache purge interval (1-720 minutes or 0 to disable) [10]
Enable transparent caching? [Yes]:
Check cache control headers? [Yes]:
Cache images? [Yes]:
    Default expiration time for images
    (1-10080 minutes or 0 for no expiration) [60]?
Cache non-image static objects? [Yes]:
    Default expiration time for non-image static objects
    (1-10080 minutes or 0 for no expiration) [60]?
URL mask to identify dynamic objects [*/cgi*]?
Cache dynamic objects? [No]:
Do you want to add a URL mask? [No]:

Cache partition number 1 has been successfully created.
Requested port has been added to cluster 113.3.1.10
Maxweight has been set to 20 for port 80 in cluster 113.3.1.10
NDR Config>add server
Cluster Address [0.0.0.0] ? 113.3.1.10
Port number [80] ? 80
Server Address [0.0.0.0] ? 113.1.2.0
Server weight [20] ?
Server state (down=0, up=1) [1] ?
Server 113.1.2.0 has been added to the requested port(s) of cluster 113.3.1.10
Weight of server 113.1.2.0 has been set to 20 in port 80 of cluster 113.31.10
Server 113.1.2.0 has been set up.
NDR Config> exit
```

A continuación se listan los parámetros del ejemplo y sus descripciones.

cluster-address Especifica la dirección IP del cluster.

Nota: Se supone que las Direcciones IP de cluster se encuentran en la misma subred lógica que el direccionador de salto (direccionador IP) anterior.

Valores válidos: cualquier dirección IP válida

Valor por omisión: 0.0.0.0

FIN-count Especifica el número de conexiones que deben estar en estado FIN antes de que el ejecutor intente eliminar la información de conexión no utilizada de la base de datos de Network Dispatcher,

Configuración y supervisión de la Antememoria del servidor de la web

después de que haya transcurrido el tiempo indicado en *FIN-timeout* o *Stale-timer*.

Valores válidos: de 0 a 65535

Valor por omisión: 4000

FIN-timeout Especifica el número de segundos que una conexión ha permanecido en el estado FIN, después de lo cual el ejecutor intenta eliminar la información de conexión no utilizada de la base de datos de Network Dispatcher.

Valores válidos: de 0 a 65535

Valor por omisión: 30

Stale-timer Especifica el número de segundos que una conexión ha permanecido inactiva, después de lo cual el ejecutor intenta eliminar la información de la conexión de la base de datos de Network Dispatcher.

Valores válidos: de 0 a 65535

Valor por omisión: 1500

port# Especifica el número de puerto del protocolo para este cluster.

Valores válidos: 1 a 65535

Valor por omisión:80

port-type Especifica los tipos de tráfico IP en los que se puede establecer el equilibrio de carga en este puerto. Los tipos soportados son:

- 1 = TCP
- 2 = UDP
- 3 = ambos

Valores válidos: 1, 2, 3

Valor por omisión: 3

max-weight Especifica el peso máximo de los servidores en este puerto. Esto afecta al grado de diferencia que puede existir entre el número de peticiones que el ejecutor proporcionará a cada servidor.

Valores válidos: 0 a 100

Valor por omisión: 20

port-mode Especifica si el puerto proveerá todas las peticiones de un único cliente a un único servidor (conocido como "sticky"), utilizará el ftp pasivo (pftp), utilizará la Antememoria del servidor de la web (cache), proveerá una matriz de antememoria escalable externa (extcache), o no utilizará ningún protocolo en particular en este cluster (none).

Valores válidos: 0 - 4, donde:

- 0 = none
- 1 = sticky
- 2 = pftp
- 3 = cache

Configuración y supervisión de la Antememoria del servidor de la web

- 4 = extcache

Valor por omisión: 0

Do you want a new cache partition? (¿Desea una nueva partición de antememoria?) Especifica si desea utilizar una partición de antememoria existente o una nueva partición.

Valores válidos: Yes o No

Valor por omisión: Yes

Enter cache partition (Entrar partición de antememoria) Especifica el número de la partición de antememoria existente que se va a utilizar.

Valores válidos: cualquier número de partición de antememoria existente

Valor por omisión: 0

Default server TCP connection timeout (Tiempo de espera de conexión TCP de servidor por omisión) Especifica la hora antes de que caduque una conexión de servidor.

Valores válidos: de 5 a 240 segundos

Valor por omisión: 120 segundos

Do you want to modify cache partition? (¿Desea modificar la partición de antememoria?) Permite modificar la configuración de una partición de antememoria existente.

Valores válidos: Yes o No

Valor por omisión: No

Default client TCP connection timeout (Tiempo de espera de conexión TCP de cliente por omisión) Especifica la hora antes de que caduque una conexión de cliente.

Valores válidos: de 5 a 240 segundos

Valor por omisión: 120 segundos

Maximum partition size (Tamaño máximo de partición) Especifica la cantidad máxima de memoria que va a asignarse a esta partición de antememoria. Si este valor sobrepasa la cantidad de memoria disponible actualmente, se pasará por alto y no se impondrá ningún tamaño máximo de partición.

Valores válidos: de 1 a 4095 Megabytes ó 0 (sin máximo)

Valor por omisión: 0 (sin máximo)

Maximum number of objects (Número máximo de objetos) Especifica el número máximo de objetos que pueden almacenarse en una partición de antememoria. Si el usuario entra un 0, la partición de antememoria sólo estará limitada por la cantidad de memoria disponible en la partición.

Valores válidos: 1 a 100000 ó 0 (sin límite)

Valor por omisión: 0 (sin límite)

Configuración y supervisión de la Antememoria del servidor de la web

Maximum object size (Tamaño máximo de objeto) Especifica el tamaño máximo de los objetos que deben incluirse en la antememoria. Los objetos que sobrepasen este tamaño máximo no se incluirán nunca en la antememoria. Si se modifica el tamaño máximo del objeto después de haber llenado la antememoria, es posible que los objetos que ya se encuentren en la antememoria puedan sobrepasar temporalmente el valor máximo definido.

Valores válidos: de 512 a 300000 bytes ó 0 (sin tamaño máximo)

Valor por omisión: 0 (sin tamaño máximo)

Do you want the cache activated upon reboot? (¿Desea que se active la antememoria al rearrancar?) Especifica si se debe activar una partición de antememoria automáticamente o tras una petición de usuario explícita. Las particiones de antememoria que están definidas para su activación inmediata se habilitan automáticamente cuando se rearranca el 2216. Las particiones de antememoria que no estén definidas para su activación inmediata permanecerán en estado inhabilitado hasta que el usuario active la partición de la consola de la Antememoria del servidor de la web en talk 5.

Valores válidos: Yes o No

Valor por omisión: Yes

Default cache purge interval? (¿Intervalo de depuración de antememoria por omisión?) Especifica el intervalo de depuración de antememoria por omisión.

Valores válidos: de 1 a 720 minutos, ó 0 (inhabilitar)

Valor por omisión: 10 minutos

Enable transparent caching? (¿Habilitar la colocación en antememoria transparente?) Especifica si se colocarán en antememoria automáticamente las respuestas del servidor para los objetos que no se encuentren en la antememoria (objetos ausentes de la antememoria).

Valores válidos: Yes o No

Valor por omisión: Yes

Check cache control headers? (¿Comprobar cabeceras de control de antememoria?) Permite a un servidor especificar a la Antememoria del servidor de la web si la respuesta es elegible para colocarse en antememoria o no.

Valores válidos: Enabled (Habilitado) o Disabled (Inhabilitado)

Valor por omisión: Disabled

Cache images? (¿Colocar imágenes en antememoria?) Especifica si se deben colocar en antememoria los archivos de imagen (*.gif o *.jpg).

Valores válidos: Yes o No

Valor por omisión: Yes

Default expiration time for images (Tiempo de caducidad por omisión para imágenes)

Valores válidos: de 1 a 10080 minutos, ó 0 (ninguno)

Valores por omisión: 60 minutos

Cache non-image static objects? (¿Colocar en antememoria los objetos estáticos que no son imágenes?) Especifica si los datos estáticos que no son imágenes (los archivos que no contienen */cgi* y los archivos que no terminan en .jpg o .gif) deben colocarse en antememoria.

Valores válidos: Yes o No

Valor por omisión: Yes

Default expiration time for non-image static objects (Tiempo de caducidad por omisión para objetos estáticos que no son imágenes)

Valores válidos: de 1 a 10080 minutos, ó 0 (ninguno)

Valores por omisión: 60 minutos

URL mask to identify dynamic objects (Máscara de URL para identificar objetos dinámicos) Especifica la máscara de URL utilizada para identificar objetos dinámicos.

Valores válidos: cualquier máscara de URL

Valor por omisión: */cgi*

Cache dynamic objects? (¿Colocar en antememoria los objetos dinámicos?) Especifica si se colocan en antememoria los objetos dinámicos. Los objetos dinámicos son aquéllos que el servidor construyó cuando se solicitó el objeto y se reconstruyen para cada petición nueva, tanto si los datos se han modificado como si no.

Valores válidos: Yes o No

Valor por omisión: No

Do you want to add a URL mask? (¿Desea añadir una máscara de URL?) Especifica una nueva máscara de URL que se debe añadir a la antememoria. Las máscaras de URL permiten al usuario incluir o excluir objetos individuales o grupos de objetos según su URL (Localizador de recursos universal).

Valores válidos: i, e

Valor por omisión: i

Los caracteres comodines pueden utilizarse al especificar una máscara de URL. Pueden utilizarse comodines al configurar Network Dispatcher para la Antememoria de Web Server o al utilizar el mandato **add** o **modify url** en el indicador **f webc**. Los caracteres utilizados como comodines son * (asterisco) o # (signo numérico). Pueden utilizarse comodines en cualquier posición como parte del URL.

El * no representa ningún carácter o bien todos los caracteres como parte de ese URL:

Configuración y supervisión de la Antememoria del servidor de la web

Ejemplo: *abc.html filtraría las siguientes máscaras de URL.

```
abc.html
finabc.html
defchtjqsprabc.html
```

representa cualquier carácter individual.

Ejemplo: ab#.html filtraría las siguientes máscaras de URL.

```
abc.html
abf.html
abo.html
```

El siguiente ejemplo es aplicable cuando se selecciona la modalidad de puerto 3 (cache=3) y no se añade una nueva partición de antememoria.

```
NDR Config>add port
Cluster Address [0.0.0.0] ? 113.3.1.11
Port number [80] ?
Max. weight (0-100) [20] ?
Only one pftp port per cluster allowed
Port mode (none=0, sticky=1 pftp=2 cache=3 extcache=4) [0] ? 3
Do you want a new cache partition? [Yes] : n
Enter cache partition [0] ? 0
Maximum TCP segment size (Range 512-32768 bytes) [4096] ?
Default server TCP connection timeout (Range 5-240 seconds) [120] ?
Default client TCP connection timeout (Range 5-240 seconds) [120] ?
Do you want to modify cache partition [0]? No :
Requested port has been added to cluster 113.3.1.11
Maxweight has been set to 20 for port 80 in cluster 113.3.1.11
```

Nota: El siguiente ejemplo es aplicable cuando se selecciona la modalidad de puerto 3 (cache=3) y se añade una nueva partición de antememoria.

```
NDR Config>add port
Cluster Address [0.0.0.0]? 113.3.1.10
Port number [80]?
Port type (tcp=1, udp=2, both=3) [3]?
Max. weight (0-100) [20]?
Only one pftp port per cluster allowed
Port mode (none=0, sticky=1 pftp=2 cache=3 extcache=4) [0]? 3
Do you want a new cache partition? [Yes]: y
Default server TCP connection timeout (Range 5-240 seconds) [120]?
Default client TCP connection timeout (Range 5-240 seconds) [120]?
Maximum partition size (1-4095 megabytes or 0 for no limit) [0]?
Maximum number of objects (1-100000 or 0 for no limit) [0]?
Maximum object size (512-300000 bytes or 0 for no limit) [0]?
Do you want the cache activated upon reboot? [Yes]:
Default cache purge interval (1-720 minutes or 0 to disable) [10]?
Enable transparent caching? [Yes]:
Check cache control headers? [Yes]:
Cache images? [Yes]:
    Default expiration time for images
    (1-10080 minutes or 0 for no expiration) [60]?
Cache non-image static objects? [Yes]:
    Default expiration time for non-image static objects
    (1-10080 minutes or 0 for no expiration) [60]?
URL mask to identify dynamic objects [*/cgi*]?
Cache dynamic objects? [No]:
Do you want to add a URL mask? [No]:

Cache partition number 0 has been successfully created.
Requested port has been added to cluster 113.3.1.10
Maxweight has been set to 20 for port 80 in cluster 113.3.1.10
Port Type has been set to Both for port 85 in cluster 113.3.1.10
NDR Config>
```

Configuración y supervisión de la Antememoria del servidor de la web

Debe utilizar Network Dispatcher para configurar el cluster y el puerto iniciales para la característica Función de colocación en antememoria del servidor de la web. Una vez que haya añadido el cluster y el puerto, configurando la *modalidad de puerto* como puerto de antememoria, podrá modificar y visualizar los parámetros de configuración de la Función de colocación en antememoria del servidor de la web en el indicador WEBC Config>.

Consulte la página 130 para obtener información acerca de Network Dispatcher.

Acceso al entorno de la Antememoria del servidor de la web

Para acceder al entorno de configuración de la Antememoria del servidor de la web, entre el siguiente mandato en el indicador Config>.

```
Config> feature webc  
WEBC Config>
```

Mandatos de la Antememoria del servidor de la web

En esta sección se describen los mandatos de configuración de la Antememoria del servidor de la web. La Tabla 19 lista los mandatos de configuración de la Antememoria del servidor de la web. Estos mandatos especifican los parámetros de la característica Antememoria del servidor de la web. Para activar estos cambios, reinicie el direccionador.

Tabla 19. Resumen de los mandatos de configuración de la Antememoria del servidor de la web

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxiv.
Activate	Activa las particiones de antememoria, utilizando la configuración más reciente.
Add	Añade una máscara de URL.
Delete	Suprime una máscara de URL o una partición.
List	Lista la información sobre la colocación en antememoria.
Modify	Modifica la información sobre la colocación en antememoria.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiv.

Activate

Utilice el mandato **activate** para inicializar todas las particiones de antememoria, utilizando la configuración más reciente.

Sintaxis:

activate

Ejemplo:

```
WEBC Config>act ?
ACTIVATE all initializes cache partitions, using
the latest configuration.
If you want to keep the active configuration, use the
ENABLE PARTITION command.
```

Add

Utilice el mandato **add** para añadir una máscara de URL.

Sintaxis:

```
add          urlmask
```

Ejemplo:

```
WEBC Config>add ur1
Partition number [0]?
New URL mask []? *newmask*
Include or Exclude from cache (i or e) [i]? i
Set default expiration time? [No]:y
Default expiration time
(1-10080 minutes or 0for no expiration) [0]? 20
The URL mask has been added to cache partition number 0.
```

Nota: Para añadir proxys y particiones, debe utilizar Network Dispatcher y ejecutar los mandatos **add port** o **set port**.

partition number (número de partición) Número de la partición que se debe añadir.

Valores válidos: cualquier número de partición válido

Valor por omisión: 0

new URL mask (nueva máscara de URL) Nombre de la máscara de URL que se debe añadir.

Valores válidos: cualquier máscara de URL.

Valor por omisión: ninguno

include or exclude from cache (incluir o excluir de antememoria) Especifica si se incluye el URL en la antememoria o se excluye de ella.

Valores válidos: i, e

Valor por omisión: i

default expiration time (tiempo de caducidad por omisión) Especifica el tiempo de caducidad por omisión, en minutos. Cero indica que no hay tiempo de caducidad.

Valores válidos: de 0 a 10080 minutos

Valor por omisión: 0 (sin tiempo de caducidad)

Delete

Utilice el mandato **delete** para suprimir una máscara de URL o una partición.

Sintaxis:

```
delete       partition
              urlmask
```

Configuración y supervisión de la Antememoria del servidor de la web

partition Número de la partición que debe suprimirse de una antememoria.

urlmask Nombre de la máscara de URL que debe suprimirse de una antememoria.

Ejemplo:

```
WEBC Config>delete url
Partition number [0]? 0
URL masks defined : 5
  1: EXCLUDE '*index*'
  2: EXCLUDE '*comp*'
  3: INCLUDE '*tmp*'
    Default expiration time: 1 minutes
  4: INCLUDE '*stat*'
    Default expiration time: 5 minutes
  5: INCLUDE '*html*'
    Default expiration time: 1000 minutes (16 hrs 40 mins)
URL mask number [1]? 5
The URL mask for cache partition number 0 has been deleted.
```

Nota: Para suprimir un proxy, debe utilizar la característica Network Dispatcher y eliminar el puerto y/o cluster asociado, o bien cambiar la modalidad de puerto del puerto de manera que no sea antememoria.

partition number (número de partición) Número de la partición que debe suprimirse.

Valores válidos: cualquier partición válida

Valor por omisión: 0

URL mask number (número de máscara de URL) Número de la máscara de URL que debe suprimirse.

Valores válidos: cualquier número de máscara de URL válido.

Valor por omisión: 1

List

Utilice el mandato **list** para listar la información sobre la Antememoria del servidor de la web.

Sintaxis:

```
list          all
                external
                partition
                proxy
                urlmask
```

all Lista todos los puertos, particiones, proxys y máscaras definidos en una antememoria.

external Lista la información del Gestor de control de antememoria externa.

partition Lista los números de partición que hay en una antememoria.

proxy Lista los proxys que están definidos en una antememoria.

urlmask Lista las máscaras de URL que están definidas en una antememoria.

Ejemplo: list all

```
WEBC Config>list all
Cache Partition 0
  Cluster address 113.3.1.10, Port 80

1 cache partition(s) defined.
```

Ejemplo: list external

```
WEBC Config>list ext
External Cache manager : Enabled
Port number            : 82
TCP timeout            : 120 seconds
```

Ejemplo: list partition

```
WEBC Config>list part
Cache Partition 0
Maximum partition size      : 1 MB
Maximum number of objects  : Unlimited
Maximum object size:      : Unlimited
Activate on reboot         : Enabled
Cache purge interval       : 10 minutes
Dynamic URL mask           : '*/cgi*' "
Transparent caching: Enabled
Check cache control headers : Disabled
Cache images               : Disabled
Cache non-image static objects: Enabled
  Default expiration time: 60 minutes (1 hrs 0 mins)
Cache dynamic objects: Disabled
Associated proxies (cluster port): (113.3.1.10 80)

1 cache partition(s) defined.
```

Ejemplo: list url

```
WEBC Config>list url
Partition number [0]?
URL masks defined : 5
  1: EXCLUDE '*index*'
  2: EXCLUDE '*comp*'
  3: INCLUDE '*tmp*'
    Default expiration time: 1 minutes
  4: INCLUDE '*stat*'
    Default expiration time: 2 minutes
  5: INCLUDE '*html*'
    Default expiration time: 1000 minutes (16 hrs 40 mins)
```

Modify

Utilice el mandato **modify** para modificar la información sobre la Antememoria de Web Server.

Sintaxis:

```
modify          external
                 partition
                 proxy
                 urlmask
```

external Permite modificar el Gestor de control de antememoria externa.

partition Permite modificar una partición.

proxy Permite modificar el proxy.

urlmask Permite modificar la máscara de URL.

Ejemplo: modify external

```
WEBC Config>mod ext
External cache manager port number(0 to disable) [82]?
TCP connection timeout (Range 5-240) seconds [120]? 20
Do you want to modify the encryption key:? [No]? Y
Encryption key should be 16 characters long.
Encryption key (16 characters) in Hex (0-9, a-f, A-F):
Encryption Key again (16 characters) in Hex (0-9, a-f, A-F):
The external cache manager has been modified.
```

external cache manager port number (número de puerto de gestor de antememoria externa) Especifica el número de puerto del gestor de control de antememoria externa que se debe modificar.

Valores válidos: 0 a 255

Valor por omisión: 82

TCP connection timeout (tiempo de espera de conexión TCP) Especifica la conexión TCP del gestor de control de antememoria externa que se debe modificar.

Valores válidos: de 5 a 240 segundos

Valor por omisión: 120

do you want to modify the encryption key (¿desea modificar la clave de cifrado?) Especifica si se debe modificar o no la clave de cifrado.

Valores válidos: yes o no

Valor por omisión: no

encryption key (clave de cifrado) La clave de cifrado del gestor de control de antememoria externa que desea modificar. La clave de cifrado debe tener una longitud de 16 caracteres y un formato hexadecimal.

Valores válidos: hexadecimales (0-9, a-f, A-F)

Valor por omisión: ninguno

Ejemplo: modify partition

```
WEBC Config>modify partition
Partition number [0] ?
Maximum partition size (1-255 megabytes or 0 for no limit) [0]? 200
Maximum number of objects (1-100000 or 0 for no limit)[0]? 5000
Maximum object size (512-300000 bytes or 0 for no limit)[0]? 250000
Do you want the cache activated upon reboot? [Yes]:
Default cache purge interval (1-720 minutes or 0 to disable) [10]? 20
Enable transparent caching? [Yes]:
Check cache control headers? [Yes]:
Cache images? [Yes]:
    Default expiration time for images
        (1-10080 minutes or 0 for no expiration) [60]?
Cache non-image static objects? [Yes]:
    Default expiration time for non-image static objects
        (1-10080 minutes or 0 for no expiration) [60]?
URL mask to identify dynamic objects [*/cgi*]? *dyn*
Cache dynamic objects? [No]: y
Cache partition number 0 has been modified.
```

partition number (número de partición) Número de la partición que debe modificarse.

Valores válidos: cualquier número de partición válido

Valor por omisión: 0

Configuración y supervisión de la Antememoria del servidor de la web

maximum partition size (tamaño máximo de partición) Tamaño máximo de la partición que debe modificarse. Cero indica que no hay límite.

Valores válidos: de 1 a 255 megabytes ó 0 para ningún límite.

Valor por omisión: 0

maximum number of objects (número máximo de objetos) Número máximo de objetos que deben modificarse en la partición. Cero indica que no hay límite.

Valores válidos: 0 a 100000 ó 0 para ningún límite

Valor por omisión: 0

maximum object size (tamaño máximo de objeto) Tamaño máximo del objeto que debe modificarse en la partición. Cero indica que no hay límite.

Valores válidos: 512 a 300000 ó 0 para ningún límite

Valor por omisión: 0

do you want the cache activated upon reboot (¿desea que se active la antememoria al rearrancar?) Especifica si se activa o no la antememoria después de rearrancar.

Valores válidos: yes o no

Valor por omisión: yes

default cache purge interval? (¿intervalo de depuración de antememoria por omisión?) Especifica el intervalo de depuración de antememoria por omisión. El valor cero inhabilita el intervalo de depuración de antememoria por omisión.

Valores válidos: 1 a 170 minutes ó 0 para inhabilitar

Valor por omisión: 10

enable transparent caching (habilitar colocación en antememoria transparente) Especifica si se debe habilitar o no la colocación en antememoria transparente.

Valores válidos: yes o no

Valor por omisión: yes

check cache control headers (¿comprobar cabeceras de control de antememoria?) Especifica si se deben comprobar o no las cabeceras de control de antememoria.

Valores válidos: yes o no

Valor por omisión: yes

cache images (imágenes de antememoria) Especifica si se deben colocar o no las imágenes en la antememoria.

Valores válidos: yes o no

Valor por omisión: yes

Default expiration time for images (Tiempo de caducidad por omisión para imágenes) Especifica el tiempo de caducidad por omisión para las imágenes. El valor cero indica que no caducan.

Valores válidos: 1 a 10080, ó 0 si no caducan

Valor por omisión: 60

cache non-image static objects (¿colocar en antememoria los objetos estáticos que no son imágenes?) Especifica si se deben colocar en la antememoria los objetos estáticos que no son imágenes.

Valor por omisión: yes

Valores válidos: yes o no

Default expiration time for non-image static objects (Tiempo de caducidad por omisión para objetos estáticos que no son imágenes) Especifica el tiempo de caducidad por omisión para los objetos estáticos que no son imágenes. El valor cero indica que no caducan.

Valores válidos: 1 a 10080, ó 0 si no caducan

Valor por omisión: 60

url mask to identify dynamic objects (máscara de URL para identificar objetos dinámicos) Especifica la máscara de URL que se debe utilizar para identificar objetos dinámicos.

Valores válidos: cualquier máscara de URL válida

Valor por omisión: */cgi*

cache dynamic objects? (¿colocar en antememoria los objetos dinámicos?) Especifica si se deben colocar en la antememoria los objetos dinámicos.

Valores válidos: yes o no

Valor por omisión: no

Ejemplo: modify url

```
WEBC Config>modify url
Partition number [0]?
URL masks defined : 5
  1: EXCLUDE '*index*'
  2: EXCLUDE '*comp*'
  3: INCLUDE '*tmp*'
    Default expiration time: 1 minutes
  4: INCLUDE '*stat*'
    Default expiration time: 2 minutes
  5: INCLUDE '*html*'
    Default expiration time: 1000 minutes (16 hrs 40 mins)
URL mask number [1] ? 4
New URL mask *stat*?
Include or Exclude from cache (i or e) [i]?
Set default expiration time? Yes :
Default expiration time
  (1-10080 minutes or 0 for no expiration) [2]? 5
URL mask number 4 has been modified.
```

partition number (número de partición) Especifica el número de partición de la URL que se debe modificar.

Valores válidos: cualquier número de partición válido

Valor por omisión: 0

url mask number (número de máscara de URL) Especifica el número de la máscara de URL que debe modificarse.

Valores válidos: cualquier número de máscara de URL válido

Valor por omisión: 1

new url mask *stat*

Valores válidos: yes

Valor por omisión: yes o no

include or exclude from cache (incluir o excluir de antememoria) Especifica si se incluye el URL modificado en la antememoria o se excluye de ella.

Valores válidos: i, e

Valor por omisión: i

set default expiration time (definir tiempo de caducidad por omisión) Especifica si se define o no el tiempo de caducidad por omisión.

Valores válidos: yes o no

Valor por omisión: yes

default expiration time (tiempo de caducidad por omisión) Especifica el tiempo de caducidad por omisión, en minutos. Cero indica que no caduca.

Valores válidos: de 1 a 10080 minutos, ó 0 si no hay caducidad.

Valor por omisión: 0

Acceso al entorno de supervisión de la Antememoria del servidor de la web

Para acceder al entorno de supervisión de la Antememoria del servidor de la web, entre **f webc** en el indicador de configuración `t 5`.

```
t 5>f webc
```

Mandatos de supervisión de la Antememoria del servidor de la web

La Tabla 20 en la página 222 lista los mandatos de supervisión de la Antememoria del servidor de la web.

Tabla 20. Resumen de los mandatos de supervisión de la Antememoria del servidor de la web

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxiv.
Activate	Activa las particiones de antememoria, utilizando la configuración más reciente.
Clear	Borra una partición o las estadísticas.
Enable	Habilita una partición.
Delete	Suprime una partición, un proxy o una máscara de URL.
Disable	Inhabilita una partición.
List	Lista la información sobre la colocación en antememoria.
Modify	Modifica la información sobre la colocación en antememoria.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiv.

Activate

Utilice el mandato **activate** para activar todas las Antememorias de Web Server o una partición o proxy específico.

Sintaxis:

activate all
 external
 partition
 proxy

all Activa todas las antememorias definidas.

external Activa el Gestor de control de antememoria externa.

partition Activa una partición de una antememoria.

proxy Activa un proxy de una antememoria.

Ejemplo: activate all

```
WEBC>act all
Cache partition 0 must be disabled to reactivate it.
Do you wish to continue? [No]: y
WEBC>
```

Ejemplo: activate Proxy

```
WEBC>act pr

1) Cluster address 113.3.1.10, Port 80, Cache partition 0
2) Cluster address 113.3.1.10, Port 81, Cache partition 0
Enter proxy number: 1 ? 1
You are trying to activate an existing proxy.
Doing this will cause the proxy to be terminated before
being reactivated.
Do you wish to continue? [No]: yes
```

Clear

Utilice el mandato **clear** para borrar una partición o unas estadísticas.

Nota: El borrado de los objetos de la partición no borra las estadísticas de la partición.

Sintaxis:

```
clear          partition  
                statistics
```

partition Borra todos los objetos de la partición.

statistics Borra las estadísticas existentes de la partición.

Ejemplo:

```
WEBC>clear partition  
Enter partition number: [0]?  
Cache partition 0 must be disabled to clear its contents.  
Do you wish to continue? [No]: yes  
Do you wish to enable this partition? [Yes]: yes
```

partition number (número de partición) Especifica el número de partición que se debe borrar.

Valores válidos: cualquier número de partición válido

Valor por omisión: 0

Enable

Utilice el mandato **enable** para habilitar una partición.

Sintaxis:

```
enable        partition
```

Ejemplo:

```
WEBC>enable partition  
Enter partition number: [0]?
```

partition number (número de partición) Número de la partición que debe habilitarse.

Valores válidos: cualquier número de partición válido

Valor por omisión: 0

Delete

Utilice el mandato **delete** para suprimir una partición.

Sintaxis:

```
delete        partition
```

partition Suprime una partición de la antememoria.

Ejemplo:

Configuración y supervisión de la Antememoria del servidor de la web

```
WEBC>delete partition
Enter partition number: [0]? 0
WARNING: This will delete partition 0 and free all memory!
Do you wish to continue? [No] : yes
WEBC>
```

partition number (número de partición) Especifica el número de partición que se debe suprimir.

Valores válidos: cualquier número de partición válido

Valor por omisión: 0

Disable

Utilice el mandato **disable** para inhabilitar una partición.

Sintaxis:

disable partition

partition Inhabilita una partición.

Ejemplo:

```
WEBC>disable partition
Enter partition number: [0]?
```

partition number (número de partición) Especifica el número de la partición que se debe inhabilitar.

Valores válidos: cualquier número de partición válido

Valor por omisión: 0

List

Utilice el mandato **list** para visualizar la información correspondiente a toda la Función de colocación en antememoria del servidor de la web, una partición, una política o un proxy.

Sintaxis:

list all
delete
depend
external
item
partition
policy
proxy

all Lista todas las particiones, políticas y proxys que hay en una antememoria.

delete Lista los 100 últimos elementos suprimidos de la partición de antememoria.

depend Lista la tabla de dependencias de la partición.

external Lista la información del Gestor de control de antememoria externa.

item Lista los elementos actuales y la cuenta de entradas en la partición de antememoria.

Configuración y supervisión de la Antememoria del servidor de la web

partition Lista la información sobre la partición en la antememoria.

policy Lista la información sobre la política en la antememoria.

proxy Lista la información sobre el proxy en la antememoria.

Ejemplo:

```
WEBC>list all
Cache Partition 0      Status: Enabled
      Cluster address: 113.3.1.10 Port 80
1 partition(s) active.
External Cache Manager Port: 82
      Connection Timeout: 120 seconds
```

Ejemplo:

```
WEBC>list delete
Enter partition number: [0]? 0
Delete Table
URL String -- hit count
=====
'/abc.html' -- 4
'/soccer.html' -- 2
'/tennis.html' -- 1
'/curling.html' -- 3
```

Ejemplo:

```
WEBC>list depend
Enter partition number: [0]?
Dependency table for Partition 0
-----
dep: tennis_info
  count of URLs: 2
  URLs:
    tennis_schedule.html
    tennis_roster.html
dep: soccer_info
  count of URLs: 2
  URLs:
    soccer_schedule.html
    soccer_roster.html
dep: roster
  count of URLs: 2
  URLs:
    soccer_roster.html
    tennis_roster.html
dep: schedule
  count of URLs: 2
  URLs:
    soccer_schedule.html
    tennis_schedule.html
```

Ejemplo:

```
WEBC>list item
Enter partition number: [0]? 0
Current number of items: 5
URL String -- hit count
=====
'/' -- 2
'/file5k.html' -- 1
'/file4k.html' -- 1
'/file2k.html' -- 3
'/file1k.html' -- 1
```

Ejemplo:

```
WEBC>1i part 0
Cache Partition 0      Status: Enabled
  Cluster address: 113.3.1.10, Port 80
  Cluster address: 113.3.1.10, Port 81
Partition size: Current - 0 bytes Highest - 0 bytes Maximum - Unlimited
Number of objects: Current - 0 Highest - 0 Maximum - Unlimited
Maximum object size: Unlimited
Cache purge interval: 10 minute(s)
Hit ratio: 0%
Total number of hits: 0
Total number of misses: 0
Object Excluded (Object too large):      0
      (Object expired):                  0
      (DONT CACHE header):              0
      (URL excluded):                    0
      (Image excluded):                  0
      (Static object excluded):          0
      (Dynamic object excluded):         0
      (Cache disabled):                  0
Objects explicitly Included: 0
Total number of purged objects: 0
Purged objects (Cache full): 0
      (Object stale): 0
      (Purged by user): 0
      (Invalidation): 0
```

Ejemplo:

```
WEBC>1i po1
Enter partition number: [0]?
Transparent caching: Enabled
Cache Control Headers: Enabled
Cache images: Enabled
  Default lifetime: 0 minute(s)
Cache non-image static objects: Enabled
  Default lifetime: 0 minute(s)
Cache dynamic objects: Disabled
Dynamic URL mask: *dyn*
URL masks defined:
  1: EXCLUDE *index*
  2: EXCLUDE *comp*
  3: INCLUDE *tmp*
      Default expiration time: 1 minutes
  4: INCLUDE *stat*
      Default expiration time: 2 minutes
  5: INCLUDE *html*
      Default expiration time: 1000 minutes (16 hrs 40 mins)
```

Ejemplo: un proxy que forma parte de la matriz de la antememoria.

```
WEBC>li pr
WEBC>li pr
  1) Cluster address 113.3.3.10, Port 80, Cache Partition 0
  2) Cluster address 113.3.3.20, Port 80, Cache Partition 0
Enter proxy number: [1]? 1
Proxy 1: assigned to cache partition 0
Cluster address: 113.3.3.10 Port number: 80
Server Connection Timeout : 120 seconds
Client Connection Timeout : 120 seconds
Client connections: 0 current / 2 at highest point
Server connections: 0 current / 2 at highest point
Total cache hits: 0
Total cache misses: 649
Cache misses (object not in cache): 649
      (unsupported method): 0
      (can't send response): 0
      (non-cached request): 0
This Proxy is part of a cache group
Source IP address for group is: 113.3.3.1
There are currently 2 Cache(s) in this group
Below are the Caches in the group:
113.3.1.1
113.3.6.1
```

Ejemplo: un proxy que no forma parte de la matriz de la antememoria.

```
WEBC>li pr
  1) Cluster address 113.3.1.10, Port 80, Cache Partition 0
  2) Cluster address 113.3.1.10, Port 81, Cache Partition 0
Enter proxy number: [1]?
Proxy 1: assigned to cache partition 0
Cluster address: 113.3.1.10 Port number: 80
Server Connection Timeout: 240 seconds
Client Connection Timeout: 240 seconds
Client connections: 0 current / 0 at highest point
Server connections: 0 current / 0 at highest point
Total cache hits: 0
Total cache misses: 0
Cache misses (object not in cache): 0
      (unsupported method): 0
      (can't send response): 0
      (non-cached request): 0
      (invalidation): 0
```

Modify

Utilice el mandato **modify** para modificar el Gestor de control de antememoria externa.

Sintaxis:

modify external

Ejemplo: modify external

```
WEBC Config>mod ext
External cache manager port number(0 to disable) [82]?
TCP connection timeout (Range 5-240) seconds) [120]? 20
Do you want to modify the encryption key:? [No]? Y
Encryption key should be 16 characters long.
Encryption key (16 characters) in Hex (0-9, a-f, A-F):
Encryption Key again (16 characters) in Hex (0-9, a-f, A-F):
```

external cache manager port number (número de puerto de gestor de antememoria externa)

TCP connection timeout (tiempo de espera de conexión TCP)

**do you want to modify the encryption key (¿desea modificar la clave de
cifrado?)**

encryption key (clave de cifrado)

Configuración y supervisión del Subsistema de codificación

Las funciones de compresión y cifrado de datos están agrupadas en el Subsistema de codificación (ES). El ES proporciona acceso a los dispositivos de software de codificación para las interfaces o los protocolos y se activa automáticamente siempre que se activa un enlace para la compresión o el cifrado. El dispositivo de software consiste en el software operativo que realiza la compresión y el cifrado. Los algoritmos de compresión y de cifrado se ejecutan en el procesador del direccionador. No es necesario modificar la configuración por omisión para utilizar el dispositivo de software.

Nota: Vea “Configuración y supervisión de la compresión de datos” en la página 237 para obtener instrucciones acerca de la configuración de sesiones de compresión a través de PPP o Frame Relay, vea “Utilización y configuración de protocolos de cifrado” en la página 279 para obtener instrucciones acerca de la configuración de sesiones de cifrado a través de PPP o Frame Relay, y vea “Configuración y supervisión de la Seguridad de IP” en la página 387 para obtener instrucciones acerca de la configuración de sesiones IPsec.

La supervisión de la actividad del ES puede realizarse entrando **feature es** en el indicador de supervisión (talk 5).

Los parámetros de configuración del ES permiten limitar la cantidad de memoria utilizada por el dispositivo de software del ES. La configuración por omisión permite al ES obtener tanta memoria como sea necesaria. Para limitar la utilización de memoria, utilice el mandato **set** bajo **feature es** en el proceso de configuración (Talk 6).

Este capítulo se compone de las secciones siguientes:

- “Configuración del Subsistema de codificación”
- “Supervisión del Subsistema de codificación” en la página 231

Configuración del Subsistema de codificación

Los parámetros de configuración del ES proporcionan una manera de controlar el número de sesiones de compresión y cifrado que utilizan a la vez el dispositivo de codificación del software. El dispositivo de codificación del software es esencialmente un conjunto de bibliotecas de compresión y de cifrado que se ejecutan en el procesador del direccionador. Una sesión se compone de una conexión dúplex a través de una interfaz específica que se ha configurado para utilizar la compresión o el cifrado.

Por lo general, la codificación de datos es una operación intensiva del procesador. Al limitar el número de sesiones de codificaciones de software, la influencia de la codificación de datos en el rendimiento del direccionador puede controlarse hasta cierto punto. Como ejemplo, si el direccionador tiene 20 interfaces de marcación configuradas para la compresión y se ha determinado que comprimir más de 10 interfaces a la vez tiene efectos adversos en el rendimiento del direccionador, el número máximo de sesiones de compresión debe definirse como 10. Esto permite que 10 interfaces de las 20 utilicen la compresión.

Configuración de ES

Los requisitos de memoria del dispositivo de codificación de software también pueden constituir un motivo para limitar el número de sesiones. Cada sesión de compresión de software utiliza aproximadamente 30 KB de memoria del direccionador y una sesión de cifrado utiliza aproximadamente 2 KB. Si el ES utiliza demasiada memoria, otras funciones pueden sufrir restricciones de memoria y el rendimiento del direccionador puede verse afectado de forma adversa. Consulte “Consideraciones” en la página 240 para obtener más información.

Puede definir el número mínimo o máximo de sesiones del ES indicando el número de sesiones o especificando uno de valores siguientes: *unlimited*, *default*, o un número. Los valores *unlimited* y *default* tienen el mismo significado: estos valores permiten al direccionador dar soporte a todas las sesiones que se han activado para el cifrado o la compresión, hasta que se agota la memoria.

Nota: Ningún parámetro de configuración del ES (talk 6) se puede volver a configurar de manera dinámica. Para activar los valores de los parámetros después de modificarlos, debe volver a cargar el direccionador.

En el proceso de configuración (talk 6), entre **feature es** en el indicador `Config>` para acceder a los mandatos de configuración del ES. Aparece el indicador `ES Config>`. La Tabla 21 lista los mandatos.

Tabla 21. Mandatos de configuración del ES	
Mandato	Acción
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxiv.
List	Visualiza el valor actual de las sesiones de compresión y cifrado.
Set	Define el número máximo de sesiones de cifrado y compresión que están disponibles para todas las interfaces.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiv.

List

Utilice el mandato **list** para visualizar el valor actual de las sesiones de compresión y cifrado.

Sintaxis:

`list`

Ejemplo:

```
ES Config> list
Data Compression and Encryption System Configuration
-----

Parameters used for host-based encoding:
Compression sessions:
  Reserved at initial bootup:          0
  Maximum allowed:                    unlimited
Encryption sessions:
  Reserved at initial bootup:          0
  Maximum allowed:                    unlimited
```

Set

Utilice el mandato **set** para definir el número máximo de sesiones de cifrado o compresión de datos.

Sintaxis:

```
set          sw minimum compression-sessions n, unlimited, o default
              sw maximum compression-sessions n, unlimited o default
              sw minimum encryption-systems n, unlimited o default
              sw maximum encryption-systems n, unlimited o default
```

Nota: Las letras sw son la abreviatura de software.

software minimum compression-sessions *n, unlimited o default*

Define el número mínimo de sesiones de compresión que están disponibles para las interfaces. El direccionador reserva este número de sesiones para que siempre estén disponibles.

Valor por omisión: 0

Valores válidos: de 0 a *unlimited*; de forma alternativa, *default*

software maximum compression-sessions *n, unlimited o default*

Define el número máximo de sesiones de compresión que están disponibles para las interfaces. Una vez que se ha activado este número de sesiones, no pueden activarse nuevas sesiones.

Valor por omisión: 0

Valores válidos: de 0 a *unlimited*; de forma alternativa, *default*

software minimum encryption-sessions *n, unlimited o default*

Define el número mínimo de sesiones de cifrado que están disponibles para las interfaces. El direccionador reserva este número de sesiones para que siempre estén disponibles.

Valor por omisión: 0

Valores válidos: de 0 a *unlimited*; de forma alternativa, *default*

software maximum encryption-sessions *n, unlimited o default*

Define el número máximo de sesiones de cifrado que están disponibles para las interfaces. Una vez que se ha activado este número de sesiones, no pueden activarse nuevas sesiones.

Valor por omisión: 0

Valores válidos: de 0 a *unlimited*; de forma alternativa, *default*

Supervisión del Subsistema de codificación

En el proceso de supervisión, entre **feature es** en el indicador + para acceder a los mandatos de supervisión del ES. Aparece el indicador ES Monitor>. La Tabla 22 en la página 232 lista los mandatos disponibles.

Tabla 22. Mandato de supervisión del ES

Mandato	Acción
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxiv.
List	Lista los puertos, circuitos, dispositivos, configuración, estado o resumen de ES.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiv.

List

Utilice el mandato **list** para listar información acerca del ES. Consulte el mandato **list summary** para ver un ejemplo de la salida del mandato **list** que incluye puertos, dispositivos y estados.

Sintaxis:

```
list          ports
              circuits
              devices
              config
              status
              summary
```

ports El mandato **list ports** lista los puertos de codificación creados por clientes potenciales del sistema de codificación. Un puerto establece un enlace entre el sistema de codificación y los clientes que se han configurado para utilizar el ES. Por ejemplo, si la compresión o el cifrado se ha configurado a través de la interfaz PPP Net 1, un puerto se asociará a esa interfaz. El campo QLen muestra la suma de todas las peticiones importantes de compresión o cifrado para todos los circuitos asociados al puerto. Un cliente, como un PPP configurado a través de una interfaz determinada, presenta una petición al ES cuando designa un almacenamiento intermedio de datos específico para la codificación.

El campo Status muestra *Idle* si no se coloca nada en cola en el puerto, o bien *Busy* o *Waiting* si las peticiones están en proceso o colocadas en cola en el puerto.

circuits El mandato **list circuits** visualiza los circuitos definidos por los clientes del sistema de codificación. Cada circuito corresponde a una conexión dúplex. La fecha cifrada o comprimida en un extremo se descifra o descomprime en el otro.

Por omisión, sólo se visualizan los circuitos activos. Utilice el mandato **list circuits all** para incluir tanto los circuitos activos como los inactivos.

Para cada circuito encontrado, el puerto y el usuario se visualizan como en el mandato **list ports**. Además, se muestran dos líneas de información, una línea Tx para el circuito de salida y una línea Rx para el circuito de entrada. El ID de circuito es un número arbitrario proporcionado por el cliente, de manera que puede codificar cada circuito que crea. Para los circuitos Frame Relay, este número corresponde al ID del

circuito de enlace de datos (DLCI) Frame Relay asociado. Los enlaces Punto a punto sólo crean un circuito, que se identifica siempre con el número 1.

Además, se visualizan los elementos siguientes:

- Dev** Es el número que representa el dispositivo de codificación que da servicio a esa corriente de datos. Es 1 cuando el software que activa la CPU realiza la codificación, y 2 cuando el adaptador de compresión/cifrado realiza la codificación.
- Cmpr** Este campo visualiza el algoritmo de compresión o descompresión que está activo para esa corriente de datos. Si es *LZC*, se utiliza la compresión STAC-LZC; si es *MPPC*, se utiliza PPC de Microsoft®. Se añade un asterisco (*) al nombre del algoritmo si la corriente de datos opera en modalidad sin estado. La modalidad sin estado es aquélla en la que no se mantiene el historial del paquete de datos después de haberse procesado este paquete, a diferencia de la modalidad continua, en la que el historial se mantiene desde la gestión de un determinado paquete para poder gestionar también el siguiente. Por ejemplo, en la compresión continua, el codificador mantiene una antememoria de información reunida a partir de paquetes anteriores, con el fin de comprimir los paquetes actuales de forma más eficaz.
- Encr** Este campo visualiza el algoritmo de cifrado o de descifrado que se utiliza. Es *DES* para DES estándar, *3DES* para Triple DES, o *RC4* si se utiliza el algoritmo RC4 de RSA. Se añade un asterisco (*) al nombre si la corriente de datos opera en modalidad sin estado. Esto es relevante para RC4, pero no lo es apenas para DES/3DES. Tenga en cuenta que el nombre indicado corresponde al algoritmo de cifrado básico empleado, no al formato de encapsulación utilizado por el cliente. Por ejemplo, PPP da soporte a dos métodos de encapsulación: DESE (RFC 1969), que realiza el cifrado con DES, y MPPE (no es un estándar de Microsoft), que utiliza RC4.
- QLen** Este parámetro muestra el número de paquetes importantes colocados en la cola de la corriente de datos, a la espera de su codificación o descodificación. Tenga en cuenta que este número sólo refleja los paquetes sometidos realmente al ES para su proceso. Algunos clientes pueden mantener sus propias colas y proveer sólo algunos paquetes a la vez al sistema de codificación desde estas colas privadas.
- Status** Indicación rápida del estado de la corriente de datos. No es habitual que todas las corrientes de datos tengan el estado en espera y ninguna parezca estar ocupada. Ver el estado ocupado requiere retener la actividad de las colas durante un período de tiempo bastante reducido en el ciclo de proceso. Éstos son los estados posibles:
- Idle (Desocupado)** No hay ningún paquete en cola en esta corriente de datos

Busy (Ocupado) El sistema está procesando paquetes en esta corriente de datos (lo que quiere decir que el elemento situado en primera posición de la cola está pasando a través del motor de codificación).

Waiting (En espera) Las peticiones están pendientes, pero ningún elemento de esa corriente se está procesando en esos momentos.

devices El mandato **list devices** lista los dispositivos de codificación que el sistema tiene disponibles. Un dispositivo de codificación suele referirse a un adaptador de compresión/cifrado. El software que se utiliza cuando un acelerador de hardware no está disponible, se implementa como un dispositivo virtual y aparece también en esta lista como dispositivo de *Software de sistema principal*. Este mandato tiene dos formatos: **list devices** y **list device n**. El primer formato genera una breve lista resumen de todos los dispositivos reconocidos por el sistema. La segunda produce una lista detallada referida a un dispositivo específico n, donde n representa el número de la unidad. La unidad 1 representa el software de sistema principal, que es un dispositivo de codificación virtual, mientras que la unidad 2 representa el adaptador de compresión/cifrado. Puede utilizarse un asterisco (*) en lugar del número n, en cuyo caso se proporciona una lista para ambas unidades.

config El mandato **list config** visualiza los parámetros de configuración actuales. Son los parámetros leídos desde la memoria no volátil cuando se reinicia o se recarga el direccionador. La información visualizada es idéntica a la visualizada por el mandato de configuración **list config** (Talk 6).

status El mandato **list status** visualiza el estado de codificación, que se compone de algunos distintivos de estado global y diversas estadísticas del sistema. Éstas son las descripciones de los campos visualizados con el mandato **list status**:

Last Error

Último código de error devuelto a cualquier cliente del sistema de codificación. Está concebido para funciones de depuración y debe utilizarlo el personal de servicio técnico.

Internal Condition flags

Este campo muestra determinadas condiciones internas, tal como están definidas en la lista siguiente:

Ready El sistema está activo y operativo. Es la condición normal.

Not Working

El sistema de codificación no está operativo, debido a un error interno.

No Devices Available

Indica que ningún dispositivo está disponible para realizar la codificación. Esta condición no debe producirse, porque, si no hay un codificador basado en el hardware, el software interno realiza la codificación.

Out of Memory

El sistema ha intentado asignar memoria, pero ha habido una anomalía. Esta condición indica que el direccionador tiene una RAM baja de recursos y que el sistema de codificación se ha visto afectado de forma adversa.

Number of Ports

Este campo indica el número de clientes que han establecido puertos para su propio uso en el ES. Vea la definición del puerto en el mandato **list ports**.

Number of Circuits

Vea la definición de los circuitos en el mandato **list circuits**.

Global Request pool size

Número de almacenamientos intermedios de petición que están asignados y libres. Se utiliza aproximadamente una petición por cada paquete que se ha codificado. Si el número de almacenamientos intermedios libres es menor que el número asignado, quiere decir que se está procesando la codificación.

Total # of Requests processed

Este valor muestra el número total de almacenamientos intermedios procesados por el motor de codificación. Este número corresponde aproximadamente al número total de paquetes que todos los clientes del sistema han comprimido o cifrado desde la última vez que el direccionador se volvió a iniciar o a cargar.

summary Este mandato visualiza un resumen del sistema. Es un mandato compuesto que combina la salida de los mandatos **list status**, **list devices** y **list ports**.

Ejemplo:

list summary

Encoding System Status

Last Error: 14 (Stream not active)

Internal Condition flags: 0x00000001 -->
Ready

Number of Ports: 2

Global Request pool size: Alloc: 32 Free: 32

Total # of Requests processed: 7059

Encoding System Devices

Encoding System Devices

Device Type	Slot/Port	Status
1 Host Software	0/0	Ready
0 Null Device	0/0	Ready

Encoding System Ports

Port	User	+--Encoder State---+		+--Decoder State---+	
		QLen	Status	QLen	Status
1	Net 2 (PPP/0)	0	Idle	0	Idle
2	Net 3 (PPP/1)	0	Idle	0	Idle

Configuración y supervisión de la compresión de datos

Este capítulo analiza la compresión de datos en un 2216 a través de las interfaces Frame Relay y PPP. Contiene las siguientes secciones:

- “Visión general de la compresión de datos”
- “Conceptos de la compresión de datos”
- “Configuración y supervisión de la compresión de datos en enlaces PPP” en la página 243
- “Configuración y supervisión de la compresión de datos en enlaces Frame Relay” en la página 245

La compresión de datos está soportada en las interfaces Frame Relay y PPP.

Visión general de la compresión de datos

El sistema de compresión de datos proporciona un medio para aumentar el ancho de banda efectivo de las interfaces de red en el dispositivo. Su propósito principal es su utilización en los enlaces de WAN más lentos.

La compresión de datos en el dispositivo está soportada para las interfaces PPP y Frame Relay:

- Para las interfaces PPP, la compresión se implementa según el Protocolo de control de compresión (CCP), tal como está definido en el documento RFC 1962 del Internet Engineering Task Force. CCP proporciona los mecanismos subyacentes según los cuales se negocia el uso de la compresión, así como un medio para elegir entre varios protocolos de compresión posibles.

El dispositivo proporciona dos protocolos de compresión: el protocolo Stac-LZS, definido en el documento RFC 1974, y el protocolo MPPC (Compresión punto a punto de Microsoft), descrito en el documento RFC 2118. Ambos están basados en algoritmos de compresión proporcionados por Stac Electronics.

- Para las interfaces Frame Relay, la compresión se implementa según el FRF.9, *Data Compression over Frame Relay Implementation Agreement* publicado por el Frame Relay Forum Technical Committee. El FRF.9 describe un Protocolo de compresión de datos (DCP), modelado según el CCP de PPP y, de manera similar, proporciona un medio de negociar varios algoritmos y opciones de compresión. El dispositivo da soporte a la negociación “mode 1” de DCP. El FRF.9 describe también un “mode 2” más generalizado, que no está soportado. La compresión propiamente dicha se realiza con el mismo motor de compresión utilizado para el protocolo PPP Stac-LZS.

Conceptos de la compresión de datos

La compresión de datos en el dispositivo proporciona un medio para aumentar la productividad en los enlaces de red mediante un uso más eficiente del ancho de banda disponible en un enlace. El principio básico que subyace es sencillo: representar los datos que pasan por un enlace de la manera más compacta posible, de manera que el tiempo necesario para transmitirlos sea el más corto posible, dada una velocidad determinada en un enlace.

La compresión de datos puede realizarse en muchas capas en el modelo de red. En un extremo del espectro, las aplicaciones pueden comprimir datos antes de transmitirlos a aplicaciones similares situadas en otros puntos de la red, mientras que, en el otro extremo del espectro, los dispositivos pueden realizar la compresión en la capa de enlace de datos, que funciona únicamente en la corriente de datos que pasa entre dos nodos. La manera como se realiza esta compresión y su grado de efectividad depende de diversos factores, incluidas cosas tales como la capa de red en la que se realiza la compresión, cuánto conocimiento intrínseco tienen el compresor y el descompresor acerca de los datos que se comprimen, el algoritmo de compresión elegido y los datos reales que se comprimen. Normalmente, la mejor compresión puede realizarse en la capa de aplicación; por ejemplo, una transferencia de archivos tiene habitualmente la ventaja de tener un conjunto completo de datos disponibles antes de intentar la compresión y puede probar distintos algoritmos de compresión en el archivo para ver cuál funciona mejor con los datos de ese archivo determinado. Aunque este procedimiento puede proporcionar una compresión excelente para ese tipo de aplicación, apenas sirve para resolver el problema general de comprimir el grueso del tráfico que pasa por una red, ya que la mayoría de las aplicaciones de red no comprimen los datos a medida que los generan.

La compresión tiene lugar en el dispositivo en una capa de red mucho más baja, en la capa de enlace de datos. En el dispositivo, la compresión se realiza en los paquetes individuales que se transmiten a través de un enlace. La compresión se realiza en tiempo real, a medida que los paquetes pasan a través del dispositivo: el remitente comprime un paquete justo antes de transmitirlo y el descompresor descomprime el paquete en cuanto lo recibe. Esta operación es transparente para los protocolos de red de capas superiores.

Conceptos básicos de la compresión de datos

Los compresores de datos funcionan reconociendo la información “redundante” que hay en los datos y produciendo un conjunto de datos distinto que contiene la menor cantidad de redundancia posible. La información “redundante” es cualquier clase de información que puede derivarse y volver a crearse basándose en los datos disponibles actualmente. Por ejemplo, un compresor podría funcionar reconociendo patrones de caracteres repetidos en una corriente de datos y sustituyéndolos por una secuencia de códigos más corta que represente ese patrón. Mientras el compresor y el descompresor coincidan en el significado de estas secuencias de códigos, el descompresor siempre podrá volver a crear los datos originales a partir de los datos comprimidos.

Esta correlación entre las secuencias en los datos originales y las secuencias correspondientes en la salida comprimida suele denominarse **diccionario de datos**. Estos diccionarios pueden definirse de manera estática, como información basada en la experiencia que está disponible tanto para el compresor como para el descompresor, o bien puede generarse dinámicamente, basándose por lo general en la información que se comprime. Los diccionarios estáticos son aplicables preferentemente a los entornos en los que los datos que se procesan son de naturaleza conocida y limitada, mientras que no son muy eficaces con los compresores de carácter general. La mayoría de los sistemas de compresión utilizan diccionarios dinámicos, incluidos los compresores que se utilizan en el dispositivo. En un 2216, los diccionarios de datos se basan en el paquete que se procesa actualmente y posiblemente en paquetes examinados con anterioridad, pero no tienen la capacidad de realizar una “consulta anticipada” de la corriente de datos, como cuando

la compresión se realiza en otras capas. Para los sistemas en los que el diccionario de datos se deriva dinámicamente y sólo se basa en datos examinados anteriormente, el diccionario suele conocerse también como *historial*. Los términos "historial" y "diccionario de datos" se utilizarán de manera indistinta a lo largo del resto de este capítulo, aunque debe tenerse en cuenta que, en otros entornos, un historial es una forma específica de diccionario de datos.

El hecho de que el dispositivo utilice diccionarios dinámicos y tanto el compresor como el descompresor deban mantener sus diccionarios sincronizados, quiere decir que la compresión de datos funciona en una corriente de datos que pasa entre dos extremos. Por consiguiente, la compresión en el direccionador es un proceso orientado a la conexión, en el que los extremos de la conexión son los propios compresor y descompresor. Cuando se inicia la compresión en la corriente de datos, ambos extremos restablecen sus diccionarios de datos a un estado inicial conocido, que actualizan posteriormente a medida que se reciben los datos.

La compresión podría realizarse en cada paquete individual, si se restablecen los historiales antes de procesar cada paquete. Sin embargo, normalmente los diccionarios de datos no se restablecen entre los paquetes, lo que quiere decir que los historiales no se basan sólo en el contenido del paquete actual, sino también en los contenidos de los paquetes examinados anteriormente. Esto suele mejorar la eficacia general de la compresión, ya que aumenta la cantidad de datos en la que busca el compresor para eliminar redundancias. Como ejemplo, se puede analizar el caso de un sistema principal que ejecuta "ping" en otro sistema principal con IP: se envía una serie de paquetes, cada uno de los cuales es, por lo general, casi idéntico al último que se ha enviado. El compresor puede tener escasa fortuna al comprimir el primer paquete, pero puede reconocer que cada paquete posterior es muy parecido al último que ha enviado, y producir así unas versiones muy comprimidas de dichos paquetes.

Dado que los historiales del compresor y del descompresor cambian con cada paquete recibido, los mecanismos de compresión son sensibles a los paquetes perdidos, dañados o reordenados. Los protocolos de compresión empleados por el dispositivo incluyen mecanismos de señalización, por los cuales el compresor y el descompresor puede detectar la pérdida de la sincronización y resincronizarse mutuamente; esto podría ser necesario cuando se pierde un paquete debido a un error de transmisión. Lo habitual es que esto se realice incluyendo un número de secuencia en cada paquete que el descompresor comprobará para asegurarse de que recibe todos los paquetes en el orden correcto. Si detecta un error, se restablecerá a un estado inicial conocido, enviará una señal al compresor para que haga lo mismo y después esperará (descartando los paquetes comprimidos que lleguen) hasta que el compresor envíe la señal de que también se ha restablecido.

La compresión en un enlace suele realizarse en los datos que pasan por el enlace en ambas direcciones. Normalmente, en cada extremo de una conexión se ejecutan un compresor y un descompresor, que se comunican con sus análogos en el otro extremo de la conexión tal como se muestra en la Figura 20 en la página 240. El lado de la salida (compresión) se ejecuta de manera independiente al de la entrada (descompresión). Es posible que operen algoritmos de compresión totalmente diferentes para cada dirección del enlace. Cuando se establece una conexión de enlace, el protocolo de control de compresión del enlace negociará con su similar para determinar los algoritmos de compresión que se utilizarán para la conexión. Si ambos extremos no pueden ponerse de acuerdo en los protocolos de compresión que se utilizarán, no se realizará la compresión y el enlace funcio-

ará con normalidad: simplemente, los paquetes se enviarán en formato no comprimido.

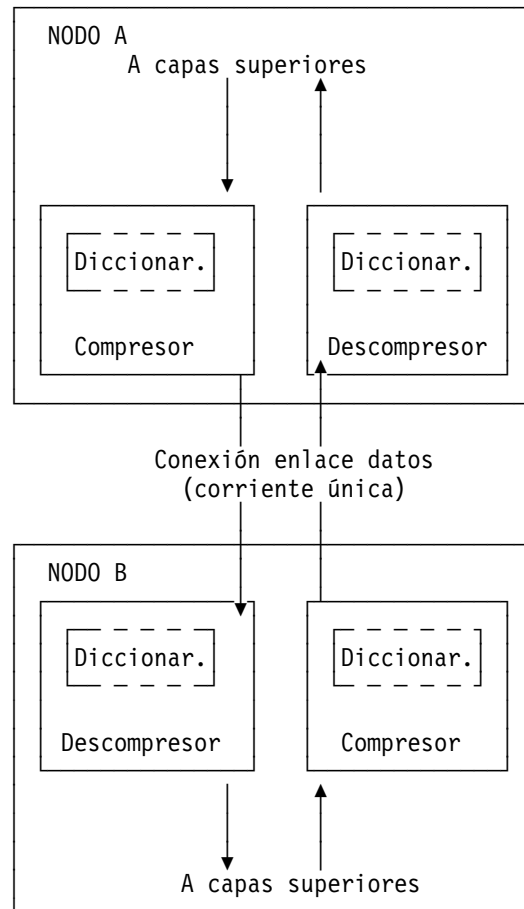


Figura 20. Ejemplo de compresión de datos bidireccional con diccionarios de datos

En realidad, una corriente representa una conexión entre un proceso de compresión específico en un extremo de un enlace y un proceso de descompresión asociado en el otro extremo; por lo tanto, es más específico que una simple “conexión” entre dos nodos; es posible que un protocolo de compresión sofisticado pueda dividir en varias corrientes los datos que pasan entre dos sistemas principales, comprimiendo cada corriente de manera independiente. Por ejemplo, el CCP de PPP tiene la capacidad de negociar el uso de varios historiales a través de un único enlace PPP, aunque no está soportada por el direccionador.

Consideraciones

No siempre es fácil la elección entre utilizar la compresión de datos o no. Hay varios factores que deben tenerse en cuenta antes de habilitar la compresión en una conexión.

Carga de la CPU

La compresión de datos es un procedimiento costoso, desde el punto de vista computacional. A medida que aumenta la cantidad de datos que se comprimen (por unidad de tiempo), se pone una carga mayor en el procesador del dispositivo. Si la carga es demasiado grande, el rendimiento del dispositivo bajará en todas las interfaces de red, no sólo en aquéllas donde se realiza la compresión.

El dispositivo contiene realmente varios procesadores y utiliza el multiproceso asimétrico -por ejemplo, enlazar controladores de E/S que operan en tándem con el procesador principal-, por lo que el efecto de la carga del procesador no siempre puede medirse fácilmente. Dado que la operación de compresión puede solaparse con la transmisión de paquetes, esta carga, de hecho, puede ser totalmente transparente y no presentar ningún problema. De todas formas, es posible que se sobrecargue el procesador del dispositivo y que el rendimiento empeore.

Como regla general, sólo debe habilitarse la compresión en los enlaces WAN de velocidad baja, probablemente sólo para los enlaces que tengan una velocidad máxima de unos 64 kilobits por segundo (que es la velocidad de un enlace por marcación RDSI típico). El ancho de banda total para los datos que se comprimen en todos los enlaces debe limitarse probablemente a varios centenares de kilobits por segundo. Sería una mala decisión ejecutar la compresión en todos los canales de un adaptador RDSI de Velocidad primaria.

Los parámetros de Subsistema de codificación permiten limitar el número de conexiones que pueden ejecutar la compresión de manera simultánea. Pueden habilitarse más interfaces para la compresión de las que realmente la ejecutan. Una vez que se alcanza el límite en el número de conexiones de compresión activas, las conexiones adicionales no negociarán el uso de la compresión, al menos hasta que no se cierre un enlace de compresión ya existente.

Utilización de la memoria

Otro asunto que debe tenerse en cuenta al configurar la compresión es el requisito de memoria. Los historiales de compresión y descompresión ocupan una cantidad importante de memoria, que es un recurso limitado del dispositivo. Por ejemplo, el algoritmo Stac-LZS requiere unos 16 KB para un historial de compresión y unos 8 KB para un historial de descompresión. Este problema se agrava por el hecho de que estos historiales deben existir para cada conexión establecida; un historial de compresión se sincroniza con el historial de descompresión correspondiente en un direccionador similar. Para un enlace PPP, esto implica que debe haber un historial de compresión y otro de descompresión (suponiendo que la compresión de datos se ejecutan de manera bidireccional en el enlace). En un enlace Frame Relay, se podrían necesitar muchos historiales: un par por cada conexión virtual (DLCI) establecida.

Al arrancar, el dispositivo crea una agrupación de historiales de compresión y de descompresión. Éstos se asignan siempre por parejas, conocidas como **sesiones de compresión**: una sesión no es más que un historial de compresión emparejado con un historial de descompresión. Técnicamente, la compresión y la descompresión son funciones distintas, pero en la práctica la compresión se ejecuta casi siempre de manera bidireccional, por lo que la memoria se gestiona y se configura en términos de sesiones en vez de hacerlo como historiales individuales, como una forma de simplificar el funcionamiento. Dado que distintos algoritmos de compresión tienen diferentes requisitos de memoria para la compresión y la descompresión, la sesión adopta un tamaño aproximado de 30 KB para poder

gestionar las operaciones incluso en las peores condiciones. La agrupación de sesiones de compresión se llena según la configuración de la característica Subsistema de codificación. Vea “Configuración y supervisión del Subsistema de codificación” en la página 229 para obtener más detalles.

Siempre que el dispositivo intenta establecer una conexión de compresión en un enlace, empieza reservando una sesión de la agrupación de sesiones asignada. Si no hay ninguna sesión disponible, la compresión no se realiza en esa conexión. El direccionador puede tratar de iniciar la compresión en esa conexión posteriormente, cuando haya sesiones disponibles.

El número de sesiones de compresión que se asignan es un parámetro configurable. La definición del número de sesiones asignadas limita la cantidad de memoria utilizada y el número máximo de conexiones que pueden operar simultáneamente con la compresión. La limitación del número de conexiones de compresión que operan simultáneamente proporciona un medio que ayuda a controlar el problema de la carga de la CPU.

Contenido de datos

La naturaleza real de los datos que se transmiten en una conexión debe tenerse en cuenta antes de habilitar la compresión para esa conexión. La compresión funciona mejor en algunos tipos de datos que en otros. Los paquetes que contienen mucha información casi idéntica como, por ejemplo, un conjunto de paquetes generados a partir de un “ping” de IP, normalmente realizan la compresión de forma excelente. Una típica variedad de texto al azar y datos binarios que pasan a través de un enlace suele comprimirse en proporciones de 1,5:1 a 3:1. Algunos datos no se comprimen bien en ningún caso. En particular, los datos comprimidos raras veces pueden comprimirse aún más. De hecho, los datos que se han comprimido anteriormente pueden expandirse cuando pasan a través del motor de compresión.

Si se conoce por adelantado que la mayoría de los datos que pasan por una conexión se compondrán de datos comprimidos, se recomienda que no se habilite la compresión para esa conexión. Un ejemplo en el que puede producirse esto es una conexión con un sistema principal que se ha configurado para ser principalmente un sitio FTP de archivado de archivos, donde se almacenan todos los archivos disponibles para su transferencia en formato comprimido en el sistema principal.

Compresión de capa de enlaces

Un último factor que se debe tener en cuenta es la naturaleza del enlace de red entre dos sistemas principales. La compresión podría realizarse en una capa inferior incluso que las interfaces de hardware del dispositivo. En particular, muchos módems modernos incorporan mecanismos de compresión de datos en el hardware y en el firmware. Si se realiza la compresión en el enlace en una capa inferior (externa al dispositivo), es preferible no habilitar la compresión de datos en el dispositivo para esa interfaz. Como ya se ha mencionado, la compresión de una corriente de datos ya comprimida suele ser ineficaz y, de hecho, puede empeorar ligeramente el rendimiento. A menos que haya un motivo determinado para creer que el direccionador realizará un trabajo de compresión mucho mejor que el hardware del enlace, es mejor dejar que sea el hardware del enlace el que realice la compresión.

Configuración y supervisión de la compresión de datos en enlaces PPP

El 2216 utiliza el Protocolo de control de compresión (CCP) de PPP para negociar el uso de la compresión en un enlace. CCP proporciona un mecanismo generalizado para negociar el uso de un protocolo de compresión determinado, posiblemente hasta con un protocolo diferente en cada dirección del enlace, así como diversas opciones específicas del protocolo. El software da soporte a los protocolos Stac-LZS y MPPC, de manera que el similar también debe proporcionar soporte para uno de estos algoritmos por lo menos para negociar satisfactoriamente la compresión de datos entre ambos nodos. Los nodos deben estar de acuerdo también en las opciones específicas de los algoritmos para que opere la compresión.

Configuración de la compresión de datos en enlaces PPP

Para configurar la compresión de datos en enlaces PPP:

1. Habilite el protocolo CCP en el enlace con el mandato **enable ccp**. Esto habilita el enlace para negociar la compresión con el otro nodo. La negociación incluye el algoritmo de compresión que se utilizará y las opciones específicas del protocolo.
2. Seleccione cuáles algoritmos de compresión pueden negociarse mediante el mandato **set ccp algorithms**.
3. Defina los parámetros negociables para cada algoritmo de compresión mediante el mandato **set ccp options**.

Puede visualizar la configuración de compresión actual mediante el mandato **list ccp**.

La Tabla 23 lista los mandatos disponibles y la Figura 21 en la página 244 es un ejemplo de la configuración de la compresión en un enlace PPP. Para obtener descripciones detalladas de estos mandatos, consulte el apartado 'Point-to-Point Configuration Commands' del manual *Nways Multiprotocol Access Services Guía del usuario de software*.

Mandatos de compresión de datos	Acción
disable ccp	Inhabilita la compresión de datos.
enable ccp	Habilita la compresión de datos.
set ccp options	Define las opciones del algoritmo de compresión.
set ccp algorithms	Especifica una lista con prioridades de los algoritmos de compresión.
list ccp	Visualiza la configuración de la compresión.

```

Config>net 6 1
PPP 6 Config>enable ccp
PPP 6 Config>set ccp alg 2
Enter a prioritized list of compression algorithms (first is preferred),
all on one single line.
Choices (can be abbreviated) are:
STAC-LZS MPPC
Compressor list [STAC-LZS]? stac mppc
PPP 6 Config>set ccp options
STAC: check mode (0=none, 1=LCB, 2=CRC, 3=Seq, 4=Ext) [3]?
STAC: # histories [1]?
PPP 6 Config>li ccp

CCP Options
-----
Data Compression enabled
Algorithm list: STAC-LZS MPPC
STAC histories: 1
STAC check_mode: SEQ

MPPE Options
-----
MPPE disabled
Optional encryption
Key generation: STATEFUL

```

Figura 21. Ejemplo de configuración de la compresión en un enlace PPP

Notas:

1. El mandato de red selecciona la interfaz de red para el enlace PPP. Si el enlace es un circuito de marcación PPP, debe utilizar el mandato **encapsulador** para acceder al menú de configuración de PPP.
2. Si habilita CCP y no define algoritmos para el enlace, el software define automáticamente el enlace para utilizar los protocolos STAC y MPPC, como si hubiese entrado el mandato **set ccp algorithms stac mppc**.
Si define varios algoritmos, su orden determina la preferencia de negociación para el enlace.
Si entra **set ccp algorithms none**, el software inhabilitará automáticamente la compresión en el enlace.
Si MPPE y CCP están habilitados, MPPC es el algoritmo de compresión.

Supervisión de la compresión de datos en enlaces PPP

Supervise la compresión como lo haría con otros componentes PPP. El apartado 'Accessing the Interface Monitoring Process' del manual *Nways Multiprotocol Access Services Guía del usuario de software* describe cómo acceder al entorno de consola PPP y los detalles acerca de los mandatos. La Tabla 24 lista los mandatos relacionados con la compresión. La Figura 22 en la página 245 muestra un ejemplo de lista de compresión en una interfaz PPP.

Tabla 24. Mandatos de supervisión de la compresión de datos PPP	
Mandato	Función
list control ccp	Lista el estado de CCP y las opciones negociadas.
list ccp	Lista las estadísticas de paquete CCP.
list cdp o list compression	Lista las estadísticas de datagrama comprimidas.


```

+ network 1
PPP > list control ccp

CCP State:          Open
Previous State:    Ack Sent
Time Since Change: 2 minutes and 52 seconds

Compressor:  STAC-LZS histories 1, check_mode SEQ
Decompressor: STAC-LZS histories 1, check_mode SEQ
MPPE:        Not negotiated

PPP > list ccp

CCP Statistic      In          Out
-----
Packets:           2            3
Octets:            18           27
Reset Reqs:        0            0
Reset Acks:        0            0
Prot Rejects:     1            -

PPP > list cdp

Compression Statistic  In          Out
-----
Packets:               19541       19542
Octets:                2550673    2740593
Compressed Octets:    821671     899446
Incompressible Packets: 0            0
Discarded Packets:    0            -
Prot Rejects:         0            -
Compression Ratios:   3.11        3.24

```

Figura 22. Supervisión de la compresión en una interfaz PPP

Configuración y supervisión de la compresión de datos en enlaces Frame Relay

Después de configurar los parámetros de compresión globales y habilitar la compresión en la interfaz, debe definir los parámetros para cada circuito (PVC) individual en la interfaz Frame Relay. Cada circuito definido para la interfaz puede tener la compresión habilitada en el circuito y cada circuito que negocia satisfactoriamente el uso de la compresión utiliza una sesión de compresión de la agrupación global. También puede inhabilitar la compresión en la interfaz, lo que significa que ningún circuito de esa interfaz puede elegirse para transportar el tráfico de datos comprimidos.

Configuración de la compresión de datos en enlaces Frame Relay

Para configurar la compresión de datos en enlaces FR:

1. Habilite la compresión en la interfaz mediante el mandato **enable compression**. Esto habilita el enlace para negociar la compresión con el otro nodo.
2. Habilite la compresión en cada nuevo PVC que transportará datos comprimidos con el mandato **add permanent-virtual-circuit**. Puede cambiar los PVC existentes mediante el mandato **change permanent-virtual-circuit**.

Puede visualizar la configuración de compresión actual mediante los mandatos **list lmi** o **list permanent-virtual-circuit**.

La Tabla 25 en la página 247 lista los mandatos disponibles para configurar la compresión en un enlace Frame Relay y la Figura 23 en la página 246 es un ejemplo de la configuración de un enlace Frame Relay. Vea el apartado “Frame Relay Configuration Commands” del manual *Nways Multiprotocol Access Services Guía del usuario de software* para obtener más detalles.

```

Config> net 2

Frame Relay user configuration

FR Config> enable compression
Maximum number of run-time compression circuits (zero means no limit) [0]? 0
Do you want orphan PVCs to perform compression [Y]? n
The number of currently defined non-compression PVCs is 4
Would you like to change them all to compression PVCs [N]? y

FR Config> add perm

Circuit number [16]? 22
Committed Information Rate (CIR) in bps [65536]?
Committed Burst Size (Bc) in bits [64000]?
Excess Burst Size (Be) in bits [0]?
Assign circuit name []? cir22
Is circuit required for interface operation [N]?
Do you want to have data compression performed [Y]?

FR Config>list lmi

                                Frame Relay Configuration

LMI enabled          =      No  LMI DLCI              =      0
LMI type             =      ANSI LMI Orphans OK        =      Yes
CLLM enabled         =      No  Timer Ty seconds    =      11

Protocol broadcast   =      Yes  Congestion monitoring =      Yes
Emulate multicast    =      Yes  CIR monitoring       =      No
Notify FECN source   =      No   Throttle transmit on FECN =      No

Data compression     =      Yes  Orphan compression   =      No
Compression PVC limit =      None Number of compression PVCs =      2

PVCs P1 allowed      =      64  Interface down if no PVCs =      No
Timer T1 seconds     =      10  Counter N1 increments  =      6
LMI N2 error threshold =      3  LMI N3 error threshold window =      4
MIR % of CIR         =      25  IR % Increment         =      12
IR % Decrement       =      25  DECnet length field    =      No
Default CIR          =      65536 Default Burst Size     =      64000
Default Excess Burst =      0

FR Config>list perm

Maximum PVCs allowable =      64
Total PVCs configured  =      2

Circuit Name          Circuit Number  Circuit Type  CIR in bps  Burst Size  Excess Burst
-----
circ16                 16          @ Permanent  65536      64000      0
cir22                  22          @ Permanent  65536      64000      0

* = circuit is required
# = circuit is required and belongs to a required PVC group
@ = circuit is data compression capable

```

Figura 23. Ejemplo de configuración de la compresión en un enlace Frame Relay

Tabla 25. Mandatos de configuración de la compresión de datos

Mandato	Acción
add permanent-virtual-circuit #	Se utiliza para habilitar la compresión de datos en un PVC específico que está definido en una interfaz.
change permanent-virtual-circuit #	Se utiliza para cambiar si un PVC específico comprimirá los datos o no.
disable compression	Inhabilita la compresión de datos.
enable compression	Habilita la compresión de datos.
list lmi	Visualiza la configuración actual de la interfaz.
list permanent	Lista información de resumen acerca de circuitos.

Nota: La habilitación de la compresión en los circuitos huérfanos reducirá el número de sesiones de compresión disponibles para los PVC originarios en el dispositivo.

Si habilita la compresión en una interfaz Frame Relay que ya tenga habilitada la compresión, el software le preguntará si desea modificar los parámetros de compresión en la interfaz, como se muestra en el ejemplo siguiente. Puede modificar la compresión en la interfaz sin inhabilitar la compresión.

Ejemplo de la modificación de la compresión en interfaces Frame Relay:

```
Config> net 2

Frame Relay user configuration

FR Config> enable compression
Data compression already enabled.
Do you wish to continue and change an interface parameter [Y]
Maximum number of run-time compression PVCs (zero means no limit) [0]? 32
Do you want orphan circuits to perform compression [Y]?
The number of currently defined circuits is 5
Change all of these circuits to perform compression?
```

Supervisión de la compresión de datos en enlaces Frame Relay

Supervise la compresión como lo haría con otros componentes Frame Relay. El apartado “Frame Relay Monitoring Commands” del manual *Nways Multiprotocol Access Services Guía del usuario de software* describe cómo acceder al entorno de consola Frame Relay y los detalles acerca de los mandatos. La Tabla 26 lista los mandatos relacionados con la compresión. En “Ejemplo: Supervisión de la compresión en una interfaz o circuito Frame Relay” en la página 248 se muestra un ejemplo de lista de compresión en una interfaz Frame Relay.

Tabla 26. Mandatos de supervisión de la compresión de datos Frame Relay

Mandato	Visualización
list lmi	Lista el estado actual de la interfaz.
list permanent	Lista información de resumen acerca de circuitos.
list circuit	Lista el estado actual de un circuito.

Ejemplo: Supervisión de la compresión en una interfaz o circuito Frame Relay

```
+ network 2
FR 2 > list lmi
```

Management Status:

```
-----
LMI enabled          = No   LMI DLCI              = 0
LMI type            = ANSI LMI Orphans OK         = Yes
CLLM enabled        = No
Protocol broadcast  = Yes  Congestion monitoring   = Yes
Emulate multicast   = Yes  CIR monitoring          = No
Notify FECN source = No  Throttle transmit on FECN = No
PVCs P1 allowed     = 64  Interface down if no PVCs = No
Line speed (bps)    = 64000 Maximum frame size      = 2048
Timer T1 seconds    = 10  Counter N1 increments   = 6
LMI N2 threshold    = 3   LMI N3 threshold window = 4
MIR % of CIR        = 25  IR % Increment          = 12
IR % Decrement      = 25  DECnet length field     = No
Default CIR         = 65536 Default Burst Size      = 64000
Default Excess Burst = 0

Current receive sequence = 0
Current transmit sequence = 0
Total status enquiries   = 0 Total status responses = 0
Total sequence requests  = 0 Total responses         = 0

Data compression enabled = Yes Orphan Compression     = No

Compression PVC limit    = None Active compression PVCs = 1
```

PVC Status:

```
-----
Total allowed = 64 Total configured = 1
Total active  = 1 Total congested  = 0
Total left net = 0 Total join net   = 0
```

```
FR 2 > list permanent
```

Circuit Number	Circuit Name	Orphan	Type/ Circuit State	Frames Transmitted	Frames Received
16	circ16	No	@ P/A	58364	58355
22	circ22	No	& P/A	58364	58355

A - Active I - Inactive R - Removed P - Permanent C - Congested
 * - Required # - Required and belongs to a PVC group
 @ - Data compression capable but not operational
 & - Data compression capable and operational

FR 2 > list circuit 22

Circuit name = circ22

Circuit state	=	Active	Circuit is orphan	=	No
Frames transmitted	=	58391	Bytes transmitted	=	2676894
Frames received	=	58383	Bytes received	=	2671009
Total FECNs	=	0	Total BECNs	=	0
Times congested	=	0	Times Inactive	=	0
CIR in bits/second	=	65536	Potential Info Rate	=	64000
Committed Burst (Bc)	=	64000	Excess Burst (Be)	=	0
Minimum Info Rate	=	16000	Maximum Info Rate	=	64000
Required	=	No	PVC group name	=	Unassigned
Compression capable	=	Yes	Operational	=	Yes
R-R's received	=	0	R-R's transmitted	=	0
R-A's received	=	0	R-A's transmitted	=	0
R-R mode discards	=	0	Enlarged frames	=	0
Decompress discards	=	0	Compression errors	=	0
Rcv error discards	=	0			
Compression ratio	=	1.00 to 1	Decompression ratio	=	1.00 to 1
Current number of xmit frames queued	=			=	0
Xmit frames dropped due to queue overflow	=			=	0

Utilización de la autenticación local o remota

La autenticación es el proceso de determinar quién es un usuario (o una entidad). La autenticación del acceso de usuario para el protocolo PPP en el 2216 amplía la flexibilidad de la gestión de perfiles de usuario en relación con los protocolos de autenticación PPP PAP, MSCHAP, CHAP y SPAP. Consulte 'Protocolos de autenticación PPP' del manual *Nways Multiprotocol Access Services Guía del usuario de software* para obtener información adicional acerca de la configuración de PAP, MSCHAP, CHAP y SPAP.

La autenticación puede configurarse localmente, o puede configurarse para consolidar la configuración de usuario mediante los servidores de autenticación disponibles en la red para dar servicio a las peticiones de autenticación en toda la red. El IBM 2216 implementa la autenticación mantenida localmente, así como los siguientes protocolos de servidor de autenticación:

- Radius
- TACACS
- TACACS+

Utilización de la Seguridad de autenticación, autorización y contabilidad (AAA)

La Seguridad de autenticación, autorización y contabilidad (AAA) se compone de protocolos configurables que permiten controlar accesos a los servicios. Puede configurar AAA para realizar la autenticación local o remota.

Puede configurar un protocolo de seguridad para tres tipos de funciones.

- Enlaces PPP
- Usuarios de inicio de sesión (Telnet/Inicio de sesión de consola)
- Túneles

La configuración se realiza definiendo un servidor primario y secundario. La información del servidor se configura y se almacena de forma separada de la configuración de AAA. Utilice un perfil de servidor con un nombre proporcionado durante la configuración.

En todas las circunstancias, no puede realizarse la contabilidad localmente y debe ser Radius o TACACS+.

La autorización sólo puede realizarse localmente o mediante la autenticación remota que utiliza Radius o TACACS+.

¿Qué es la Seguridad AAA?

La Seguridad AAA es el nombre del sistema de seguridad para este dispositivo. Incluye:

Autenticación

Proceso de identificar a un usuario. La autenticación utiliza un nombre y una contraseña para efectuar el acceso.

Utilización de la autenticación local o remota

Autorización

Proceso de determinar los servicios a los que se permite el acceso a un usuario. El proceso de autorización puede encontrar que el usuario no está autenticado. A continuación, el agente de autorización determina si a un usuario no autenticado se le permite el acceso a los servicios en cuestión.

Contabilidad

Proceso de registrar cuándo un usuario ha iniciado o detenido una sesión. Hay dos tipos de registros de contabilidad que están soportados.

Iniciar registros

Indica que un servicio está a punto de empezar.

Detener registros

Indica que ha finalizado un servicio.

Utilización de PPP

Para el Protocolo punto a punto (PPP), puede configurar lo siguiente:

- Autenticación
- Autorización
- Contabilidad

Cada función puede tener su propio protocolo de seguridad que se configura de manera independiente.

- La definición del protocolo de autenticación no tendrá ningún efecto sobre la autorización ni la contabilidad.
- La definición del protocolo de autorización no tendrá ningún efecto sobre la autenticación ni la contabilidad.
- La definición del protocolo de contabilidad no tendrá ningún efecto sobre la autenticación ni la autorización.
- La definición de AAA como remota definirá la autenticación, la autorización y la contabilidad como remotas.
- La definición de AAA como local definirá la autenticación, la autorización y la contabilidad como locales. No puede inhabilitar la autenticación ni la autorización.

Consulte Mandatos de configuración punto a punto del manual *Nways Multiprotocol Access Services Guía del usuario de software* para obtener detalles acerca de los mandatos de configuración que se utilizan en este entorno.

Protocolos de seguridad PPP válidos

Los protocolos de seguridad PPP válidos son los siguientes:

Métodos de autenticación

Local, RADIUS, TACACS+, TACACS

Métodos de autorización

Local, RADIUS, TACACS+

Métodos de contabilidad

RADIUS, TACACS+

Tabla 27. Definir los protocolos de seguridad PPP

Acción	Autent.	Autor.	Cont.
definir AAA local	local	local	pasar por alto
definir AAA remota	remota	remota	remota
definir AUTHENT local	local	pasar por alto	pasar por alto
definir AUTHOR local	pasar por alto	local	pasar por alto
definir AUTHENT remota	remota	pasar por alto	pasar por alto
definir ACCOUNTING local	n/a	n/a	n/a
definir AUTHOR remota	pasar por alto	remota	pasar por alto
definir ACCOUNTING remota	pasar por alto	pasar por alto	remota
inhabilitar ACCOUNTING	pasar por alto	pasar por alto	inhabilitada
inhabilitar AUTHENT	n/a	n/a	n/a
inhabilitar AUTHOR	n/a	n/a	n/a

Utilización del inicio de sesión

Para la configuración de inicio de sesión de AAA, se puede seleccionar como remota o local. Si se desea la autenticación local, también debe utilizarse la autorización local. Si se selecciona la autenticación remota, debe utilizarse la autorización remota. La contabilidad no está soportada localmente, por lo que, cuando se realice localmente la autenticación y la autorización, hay que inhabilitar la contabilidad.

Atención: Antes de habilitar el inicio de sesión de la consola, guarde la configuración con el inicio de sesión de la consola inhabilitado. Si se define la autenticación de inicio de sesión en un servidor remoto utilizando Radius, TACACS o TACACS+ y el direccionador no puede alcanzar el servidor de autenticación, se deniega el acceso al direccionador. Inhabilitar el inicio de sesión de la consola impide una situación de bloqueo.

Al configurar la autenticación remota, puede definir la autorización con otro protocolo de autorización remota Radius o TACACS+, así como definir la contabilidad para utilizar Radius o TACACS+.

- La definición de AAA como local define la autenticación y la autorización como locales y se inhabilitará la contabilidad.
- La definición de AAA como remota define la autenticación, la autorización y la contabilidad como remotas.
- La definición del protocolo de autenticación como local define automáticamente el protocolo de autorización de la misma manera e inhabilita la contabilidad.
- La definición del protocolo de autenticación como remoto sólo define automáticamente el protocolo de autorización de la misma manera si el protocolo de autorización está definido como local y pasa por alto el protocolo de contabilidad.

Utilización de la autenticación local o remota

- La definición del protocolo de autorización como remoto sólo define automáticamente el protocolo de autenticación de la misma manera si el protocolo de autenticación está definido como local y pasa por alto el protocolo de contabilidad.
- La definición del protocolo de contabilidad como remoto sólo define automáticamente el protocolo de autenticación de la misma manera si el protocolo de autenticación está definido como local, y sólo define el protocolo de autorización de la misma manera si la autorización está definida como local.
- La definición del protocolo de contabilidad como inhabilitado no tiene ningún efecto en el protocolo de autenticación o de autorización.
- No se permite la inhabilitación de la autenticación o de la autorización.

Protocolos de seguridad de Inicio de sesión/Administración válidos

Los siguientes son los protocolos de seguridad de Inicio de sesión/Administración válidos:

Métodos de autenticación/autorización

Local, RADIUS, TACACS Plus

Métodos de contabilidad

RADIUS, TACACS Plus

Acción	Autent.	Autor.	Cont.
definir AAA local	local	local	inhabilitada
definir AAA remota	remota	remota	remota
definir AUTHENT local	local	local	inhabilitada
definir AUTHOR local	local	local	inhabilitada
definir AUTHENT remota	remota	remota, si local, de lo contrario pasar por alto	pasar por alto
definir AUTHOR remota	remota, si local, de lo contrario pasar por alto	remota	pasar por alto
definir ACCOUNTING remota	remota, si local, de lo contrario pasar por alto	remota, si local, de lo contrario pasar por alto	remota
inhabilitar ACCOUNTING	pasar por alto	pasar por alto	inhabilitada
inhabilitar AUTHEN	n/a	n/a	n/a
inhabilitar AUTHOR	n/a	n/a	n/a

Utilización de túneles

Defina la autenticación de túnel de la misma manera que la autorización de túnel. Cuando defina la autenticación de túnel como local o remota, puede habilitar la contabilidad. El servidor de autorización y de autenticación de túnel debe ser el mismo.

Protocolos de seguridad de túnel válidos

Los protocolos de seguridad de Túnel válidos son los siguientes:

Métodos de autenticación/autorización

Local, RADIUS

Métodos de contabilidad

RADIUS, TACACS Plus

Tabla 29. Definir los protocolos de seguridad de túnel

Acción	Autent.	Autor.	Cont.
definir AAA local	local	local	pasar por alto
definir AAA remota	remota	remota	remota
definir AUTHENT local	local	local	pasar por alto
definir AUTHOR local	local	local	pasar por alto
definir AUTHENT remota	remota	remota	pasar por alto
definir AUTHOR remota	remota	remota	pasar por alto
definir ACCOUNTING remota	pasar por alto	pasar por alto	remota
inhabilitar ACCOUNTING	pasar por alto	pasar por alto	inhabilitada
inhabilitar AUTHENT	n/a	n/a	n/a
inhabilitar AUTHOR	n/a	n/a	n/a

Normas de las contraseñas

La autenticación local permite utilizar una contraseña para controlar el acceso al inicio de sesión. La contraseña se puede comprobar con cualquiera de las siguientes normas o con todas ellas.

Nota: Las normas siguientes sólo se aplican al inicio de sesión de usuario PPP, no al inicio de sesión de consola.

- Debe tener una longitud mínima de caracteres. Defina el número de caracteres necesarios.
- Debe contener por lo menos un carácter alfabético.
- Debe contener por lo menos un carácter no alfabético.
- Debe contener un carácter no numérico en la primera posición.
- Debe contener un carácter no numérico en la última posición.
- No debe contener más de tres caracteres idénticos consecutivos que ya se utilizaron en la contraseña anterior.
- No debe contener más de dos caracteres consecutivos.
- No debe contener el ID de usuario como parte de la contraseña.
- No debe ser igual que las tres contraseñas anteriores.

Utilización de la autenticación local o remota

- Se debe modificar al cabo de un número determinado de días. Defina el número de días entre cada cambio de contraseña.
- Debe bloquearse después de un número específico de fallos de inicio de sesión. Defina el número de fallos.

Explicación de los servidores de autenticación

Un **servidor de autenticación** es un servidor de la red que valida los ID de usuario y las contraseñas para la red. Si un dispositivo está configurado para la autenticación mediante un servidor de autenticación, y el dispositivo recibe un paquete de un protocolo de autenticación, el dispositivo pasa un ID de usuario y una contraseña al servidor para su autenticación. Si el ID de usuario y la contraseña son correctos, el servidor responderá de forma positiva. A continuación, el dispositivo puede establecer comunicación con el originador de la petición. Si el servidor no encuentra el ID de usuario y la contraseña que recibe del dispositivo, responde negativamente al dispositivo. Después, el dispositivo rechaza la sesión desde la que recibió la petición de autenticación.

Soporte de SecurID

El 2216 puede autenticar clientes de marcación que utilicen SecurID con un Security Dynamics ACE/Server. Este soporte utiliza TACACS, TACACS+ o RADIUS en el ACE/Server para autenticar el cliente. Configure el cliente de marcación de la misma manera que otros clientes de marcación en el 2216.

El cliente de marcación se conecta de la manera habitual, pero utiliza el código de paso para la contraseña. El código de paso de SecurID se compone de un número PIN de 4 a n dígitos, seguido por el número de la tarjeta de señal de SecurID. (El número máximo de dígitos del PIN depende del servidor.) El ID de usuario y la contraseña pueden aparecer como:

Username:

Password:

Figura 24. Nombre de usuario y código de paso de SecurID

Cuando el ACE/Server realiza la autenticación de la conexión, puede solicitar la señal siguiente del cliente. La señal siguiente es la que viene a continuación en la tarjeta de señal. El número máximo de dígitos de la señal siguiente depende de la tarjeta de señal de SecurID que utiliza el cliente. El cliente puede entrar el código de paso y la señal siguiente cuando se le solicita la contraseña, mediante el formato `código_paso*señal`, como en el ejemplo siguiente:

Username:

Password:

Figura 25. Código de paso de SecurID con la señal siguiente

Nota: Cuando el servidor solicita al cliente que entre la señal siguiente, el cliente debe:

1. Entrar el PIN
2. Esperar una nueva señal de la tarjeta y entrar la señal
3. Entrar * seguido de la señal siguiente de la tarjeta

El administrador de ACE/Server configura las condiciones que causan que el servidor solicite la señal siguiente o el nuevo PIN.

Los clientes de marcación deben utilizar SPAP, de manera que pueden recibir alertas del sistema de autenticación cuando tienen que entrar la señal siguiente. Si el cliente no utiliza SPAP y no se conecta de forma satisfactoria, debe intentar entrar un código de paso nuevo mediante el formato código_paso*señal. Si el cliente todavía no puede conectarse satisfactoriamente, puede haber otros problemas entre el cliente y el ACE/Server.

Limitaciones

Hay las siguientes limitaciones:

- El cifrado SDI (Security Dynamics Inc.) y DES no están soportados.
- La función "Nuevo PIN" de SecurID no está soportada.
- TACACS no da soporte a las funciones "Nuevo PIN" o "Señal-Siguiente". El cliente puede especificar la señal-siguiente al iniciar la sesión, pero el servidor no la utilizará.
- Los clientes configurados para la devolución de llamada no están soportados.
- Al utilizar CHAP con TACACS o TACACS+, defina el intervalo de nuevo reto de CHAP como 0.
- No utilice CHAP al utilizar la autenticación de RADIUS.
- Los clientes pueden obtener los mejores resultados utilizando TACACS+ y SPAP.
- No está soportado el cliente DIAL Windows 3.1 con la autenticación SecurID utilizando el multienlace.
- Al utilizar la autenticación SecurID, es muy recomendable que utilice el software cliente más reciente (por ejemplo, Windows 95 u OS/2).

Utilización de la autenticación local o remota

Configuración de autenticación

Este capítulo describe la configuración y los mandatos operativos de la autenticación. Incluye las secciones siguientes:

- “Acceso al indicador de configuración de autenticación”
- “Mandatos de configuración de autenticación”

Acceso al indicador de configuración de autenticación

Para acceder al indicador `Authent config >`:

1. Entre **talk 6** en el indicador `*`.
2. Entre **feature auth** en el indicador `Config >`.

Mandatos de configuración de autenticación

La Tabla 30 contiene una lista de los mandatos disponibles en el indicador `Authent config >`.

<i>Tabla 30. Mandatos de configuración de autenticación</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 el apartado “Cómo obtener ayuda” en la página xxxiv.
Disable	Inhabilita la contabilidad de AAA.
List	Muestra los parámetros de configuración de AAA.
Login	Configura AAA para el inicio de sesión.
Nets-info	Muestra información acerca de la autenticación de PPP local.
Password-rules	Configura las reglas de las contraseñas (habilita o inhabilita).
PPP	Configura AAA para PPP.
Quickset	Configura rápidamente el método de autenticación.
Servers	Configura los servidores AAA remotos individuales.
Set	Configura los parámetros de autenticación, sin importar su tipo.
Tunnel	Configura AAA para los túneles L2TP.
User-profile	Configura los usuarios PPP locales.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiv.

Disable

Utilice el mandato **disable** para inhabilitar la contabilidad.

Sintaxis:

`disable` `accounting`

List

Utilice el mandato **list** para visualizar los parámetros de AAA.

Sintaxis:

```
list          accounting
                authentication
                authorization
                all
                config
```

```
AAA Config> list all
ppp AAA configuration...
  ppp authentication      : Radius      serv01
  authorizeAuthent       YES
  Primary server address  1.1.1.1
  Secondary server address 2.2.2.2
  Request tries          3
  Request interval       3
  Key for encryption     <notSet>
  ppp authorization      : locallist
  ppp accounting         : Disabled
tunnel AAA configuration...
  tunnel authentication  : Radius      serv01
  authorizeAuthent       YES
  Primary server address  1.1.1.1
  Secondary server address 2.2.2.2
  Request tries          3
  Request interval       3
  Key for encryption     <notSet>
  tunnel authorization   : Radius      serv01
  authorizeAuthent       YES
  Primary server address  1.1.1.1
  Secondary server address 2.2.2.2
  Request tries          3
  Request interval       3
  Key for encryption     <notSet>
  tunnel accounting      : Disabled
login AAA configuration...
  login authentication   : Radius      serv01
  authorizeAuthent       YES
  Primary server address  1.1.1.1
  Secondary server address 2.2.2.2
  Request tries          3
  Request interval       3
  Key for encryption     <notSet>
  login authorization    : Radius      serv01
  authorizeAuthent       YES
  Primary server address  1.1.1.1
  Secondary server address 2.2.2.2
  Request tries          3
  Request interval       3
  Key for encryption     <notSet>
  login accounting       : Radius      serv01
  authorizeAuthent       YES
  Primary server address  1.1.1.1
  Secondary server address 2.2.2.2
  Request tries          3
  Request interval       3
  Key for encryption     <notSet>
```



```

AAA Config> list accounting all
accounting AAA configuration...
accounting ppp          : Disabled
accounting tunnel      : Disabled
accounting login       : Radius      serv01
  authorizeAuthent     YES
  Primary server address 1.1.1.1
  Secondary server address 2.2.2.2
  Request tries        3
  Request interval     3
  Key for encryption   <notSet>
AAA Config> list accounting config
accounting ppp          : Disabled
accounting login       : Radius      serv01
accounting tunnel      : Disabled

AAA Config> list authentication all
authentication AAA configuration...
authentication ppp     : Radius      serv01
  authorizeAuthent     YES
  Primary server address 1.1.1.1
  Secondary server address 2.2.2.2
  Request tries        3
  Request interval     3
  Key for encryption   <notSet>
authentication tunnel : Radius      serv01
  authorizeAuthent     YES
  Primary server address 1.1.1.1
  Secondary server address 2.2.2.2
  Request tries        3
  Request interval     3
  Key for encryption   <notSet>

```

Login

Utilice el mandato **login** para configurar AAA para el inicio de sesión.

La Tabla 31 contiene una lista de los submandatos disponibles con el mandato **login**.

<i>Tabla 31. Submandatos de login</i>	
Mandato	Función
Disable	Inhabilita la contabilidad para el inicio de sesión.
List	Muestra los parámetros de configuración de AAA para el inicio de sesión.
Set	Define los parámetros de configuración de AAA para el inicio de sesión.

Disable

Utilice el mandato **login disable** para inhabilitar la contabilidad.

Sintaxis:

login disable accounting

List

Utilice el mandato **login list** para mostrar los parámetros de configuración de AAA.

Sintaxis:

login list all
 accounting
 authentication
 authorization
 config

Set

Utilice el mandato **login set** para configurar parámetros de autenticación.

Sintaxis:

login set aaa
 accounting
 authentication
 authorization

aaa *tipo_aut*

Define el tipo de autenticación, autorización y contabilidad. *Tipo_aut* es uno de los siguientes:

- local** Define el tipo de autenticación, autorización y contabilidad para utilizar una base de datos de usuario mantenida localmente.
- remote** Define el tipo de autenticación, autorización y contabilidad para utilizar una base de datos de usuario remota.
 - server id** Especifica el identificador de la base de datos remota.

accounting *tipo_aut*

Define el tipo de contabilidad. *Tipo_aut* es uno de los siguientes:

- remote** Define el tipo de autenticación para utilizar una base de datos de usuario remota.
 - server id** Especifica el identificador de la base de datos remota.

authentication *tipo_aut*

Define el tipo de autenticación. *Tipo_aut* es uno de los siguientes:

- local** Define el tipo de autenticación para utilizar una base de datos de usuario mantenida localmente.
- remote** Define el tipo de autenticación para utilizar una base de datos de usuario remota.
 - server id** Especifica el identificador de la base de datos remota.

authorization *tipo_aut*

Define el tipo de autorización. *Tipo_aut* es uno de los siguientes:

- local** Define el tipo de autorización para utilizar la base de datos de usuario mantenida localmente.
- remote** Define el tipo de autorización para utilizar una base de datos de usuario remota.
- server id** Especifica el identificador de la base de datos remota.

Nets-info

Utilice el mandato **nets-info** para visualizar el protocolo de autenticación PPP configurado actualmente en cada interfaz PPP.

Sintaxis:

nets-info

Password-rules

Utilice el mandato **password-rules** para configurar la contraseña (habilitar o inhabilitar).

La Tabla 32 contiene una lista de los submandatos disponibles con el mandato **password-rules**.

<i>Tabla 32. Submandatos de password-rules</i>	
Mandato	Función
Disable	Inhabilita una regla de contraseña.
Enable	Habilita una regla de contraseña.
List	Muestra el estado actual de las reglas de contraseña (habilitadas o inhabilitadas).

Disable

Utilice el mandato **password-rules disable** para inhabilitar cualquiera de las reglas de contraseña o todas ellas.

Sintaxis:

password-rules disable all

- compare-ident-prev
- change-days
- first-non-numeric
- ident-chars
- last-non-numeric
- lockout
- minimum-length
- one-alpha
- one-nonalpha
- prev-three
- userid-contained

Configuración de autenticación

compare-ident-prev

Compara la identidad del usuario anterior con la del usuario que solicita un cambio de contraseña.

change-days

Número máximo de días antes de que sea necesario efectuar un cambio de contraseña.

Valores válidos: 0 a 360

Valor por omisión: 180

first_non-numeric

El primer carácter de una contraseña no puede ser numérico.

Valores válidos: cualquier carácter no numérico

Valor por omisión: ninguno

ident-chars

No se pueden definir más de 3 caracteres utilizados en la misma posición en una contraseña anterior.

last-non-numeric

El último carácter de la contraseña no puede ser numérica.

Valores válidos: cualquier carácter no numérico

Valor por omisión: ninguno

lockout

Número de veces que se puede intentar una contraseña antes de que el usuario sea bloqueado.

Valores válidos: 0 a 360

Valor por omisión: 3

minimum-length

Número mínimo de caracteres necesarios para que una contraseña sea válida.

Valores válidos: 1 a 31

Valor por omisión: 8

maximum-length

Número máximo de caracteres que puede contener una contraseña.

Valores válidos: 1 a 31

Valor por omisión: 8

one-alpha

Por lo menos un carácter de la contraseña debe ser alfanumérico.

one-nonalpha

Por lo menos un carácter de la contraseña debe ser numérico.

prev-three

La contraseña no puede ser igual que cualquiera de las tres últimas contraseñas.

userid-contained

La contraseña no puede contener el ID de usuario como parte de ella.

Enable

Utilice el mandato **password-rules enable** para habilitar cualquiera de las reglas de contraseña o todas ellas. Vea el mandato **disable** para ver una lista de descripciones de las reglas de contraseña.

Sintaxis:

```
password-rules enable all
                        compare-ident-prev
                        change-days
                        first-non-numeric
                        ident-chars
                        last-non-numeric
                        lockout
                        minimum-length
                        one-alpha
                        one-nonalpha
                        prev-three
                        userid-contained
```

List

Utilice el mandato **password-rules list** para mostrar el estado actual de las reglas de contraseña (inhabilitadas o habilitadas).

Sintaxis:

```
password-rules list
```

PPP

Utilice el mandato **ppp** para configurar AAA para PPP.

La Tabla 33 contiene una lista de los submandatos disponibles con el mandato **ppp**.

<i>Tabla 33. Submandatos de PPP</i>	
Mandato	Función
Disable	Inhabilita la contabilidad para PPP.
List	Muestra los parámetros de configuración de AAA para PPP.
Set	Define los parámetros de configuración de AAA para PPP.

Disable

Utilice el mandato **ppp disable** para inhabilitar la contabilidad para PPP.

Sintaxis:

```
ppp disable accounting
```

Configuración de autenticación

List

Utilice el mandato **ppp list** para mostrar los parámetros de configuración de AAA para PPP.

Sintaxis:

```
ppp list      all
              accounting
              authentication
              authorization
              config
```

Set

Utilice el mandato **ppp set** para definir los parámetros de configuración de AAA para PPP.

Sintaxis:

```
ppp set      aaa
              accounting
              authentication
              authorization
```

aaa *tipo_aut*

Define el tipo de autenticación, autorización y contabilidad. *Tipo_aut* es uno de los siguientes:

- local** Define el tipo de autenticación, autorización y contabilidad para utilizar una base de datos de usuario mantenida localmente.
- remote** Define el tipo de autenticación, autorización y contabilidad para utilizar una base de datos de usuario remota.
 - server id** Especifica el identificador de la base de datos remota.

accounting *tipo_aut*

Define el tipo de contabilidad. *Tipo_aut* es uno de los siguientes:

- remote** Define el tipo de autenticación para utilizar una base de datos de usuario remota.
 - server id** Especifica el identificador de la base de datos remota.

authentication *tipo_aut*

Define el tipo de autenticación. *Tipo_aut* es uno de los siguientes:

- local** Define el tipo de autenticación para utilizar una base de datos de usuario mantenida localmente.
- remote** Define el tipo de autenticación para utilizar una base de datos de usuario remota.
 - server id** Especifica el identificador de la base de datos remota.

authorization *tipo_aut*

Define el tipo de autorización. *Tipo_aut* es uno de los siguientes:

local Define el tipo de autorización para utilizar la base de datos de usuario mantenida localmente.

remote Define el tipo de autorización para utilizar una base de datos de usuario remota.

server id Especifica el identificador de la base de datos remota.

Servers

Utilice el mandato **servers** para configurar servidores AAA remotos individuales.

La Tabla 34 contiene una lista de los submandatos disponibles con el mandato **servers**.

<i>Tabla 34. Submandatos de server</i>	
Mandato	Función
Add	Añade un perfil de servidor AAA remoto.
Change	Cambia un perfil de servidor remoto.
Delete	Suprime un perfil de servidor remoto.
Lists	Muestra la información de perfil de servidor AAA.

Add

Utilice el mandato **servers add** para añadir un perfil de servidor remoto.

Sintaxis:

servers add nombre

radius Define el tipo de autenticación para utilizar el protocolo de servidor de autenticación de radio.

Pueden definirse los valores de los siguientes parámetros:

key-for-encryption:

Especifica la clave de cifrado.

Valores válidos: Cualquier serie de caracteres alfanumérico de 32 caracteres de longitud como máximo.

Valor por omisión: ninguno.

primary-server-address:

Especifica la dirección del servidor de autenticación primario.

Valores válidos: Cualquier dirección IP válida

Valor por omisión: 0.0.0.0

retries

Valores válidos: 1 a 100

Valor por omisión: 3

retry-interval

Valores válidos: 1 a 60

Configuración de autenticación

Valor por omisión: 3

secondary-server-address:

Especifica la dirección del servidor de autenticación secundario.

Valores válidos: Cualquier dirección IP válida

Valor por omisión: 0.0.0.0

Author-Authent

Especifica si los atributos de autorización se transfieren durante la autenticación.

Valores válidos: yes, no

Valor por omisión: yes

tacacs Define el tipo de autenticación para utilizar el protocolo de servidor de autenticación TACACS.

Pueden definirse los valores de los siguientes parámetros:

primary-server-address:

Especifica la dirección del servidor de autenticación primario.

Valores válidos: Cualquier dirección IP válida

Valor por omisión: 0.0.0.0

retries

Valores válidos: 1 a 100

Valor por omisión: 3

retry-interval

Valores válidos: 1 a 60

Valor por omisión: 3

secondary-server-address:

Especifica la dirección del servidor de autenticación secundario.

Valores válidos: Cualquier dirección IP válida

Valor por omisión: 0.0.0.0

tacacsplus

Define el tipo de autenticación para utilizar el protocolo de servidor de autenticación TACACS+.

Pueden definirse los valores de los siguientes parámetros:

encryption:

Especifica si se utilizará el cifrado.

Valores válidos: yes, no

Valor por omisión:

key-for-encryption:

Especifica la clave de cifrado que se va a utilizar.

Valores válidos: Cualquier valor de dígito hexadecimal

Valor por omisión:

primary-server-address:

Especifica la dirección del servidor de autenticación primario.

Valores válidos: Cualquier dirección IP válida

Valor por omisión: 0.0.0.0

privilege-level

Valores válidos: 0 a 15

Valor por omisión: 0

restarts Define el número de reinicios. Este parámetro no incluye reinicios de tiempo de espera y sólo pertenece a los reinicios solicitados por el servidor.

Valores válidos: 0 a 3200

Valor por omisión: 0

time-to-connect

Cantidad de tiempo permitido para obtener la autenticación del servidor.

Valores válidos: 1 a 60

Valor por omisión: 9

secondary-server-address:

Especifica la dirección del servidor de autenticación secundario.

Valores válidos: Cualquier dirección IP válida

Valor por omisión: 0.0.0.0

Change

Utilice el mandato **servers change** para modificar un perfil de servidor remoto. Vea las descripciones de perfil de servidor remoto en el mandato **add**.

Sintaxis:

```
servers change radius  
tacacs  
tacacsplus
```

Vea las descripciones de perfil de servidor remoto en el mandato **servers add**.

Delete

Utilice el mandato **servers delete** para suprimir un perfil de servidor remoto. Vea las descripciones de perfil de servidor remoto en el mandato **add**.

Sintaxis:

```
servers delete radius  
tacacs
```

Configuración de autenticación

tacacsplus

Vea las descripciones de servidor remoto en el mandato **servers add**.

List

Utilice el mandato **servers list** para mostrar la información de perfil de servidor AAA.

Sintaxis:

```
servers list    all  
                 names  
                 profile
```

Set

Utilice el mandato **set** para definir los parámetros para el inicio de sesión, PPP y el túnel L2TP.

Sintaxis:

```
set            aaa  
                accounting  
                authentication  
                authorization
```

aaa *tipo_aut*

Define el tipo de autenticación, autorización y contabilidad. *Tipo_aut* es uno de los siguientes:

local Define el tipo de autenticación, autorización y contabilidad para utilizar una base de datos de usuario mantenida localmente.

remote Define el tipo de autenticación, autorización y contabilidad para utilizar una base de datos de usuario remota.

server id Especifica el identificador de la base de datos remota.

accounting *tipo_aut*

Define el tipo de contabilidad para el inicio de sesión, PPP y el túnel. *Tipo_aut* es uno de los siguientes:

remote Define el tipo de autenticación para utilizar una base de datos de usuario remota.

server id Especifica el identificador de la base de datos remota.

authentication *tipo_aut*

Define el tipo de autenticación para el inicio de sesión, PPP y el túnel. *Tipo_aut* es uno de los siguientes:

local Define el tipo de autenticación para utilizar una base de datos de usuario mantenida localmente.

remote Define el tipo de autenticación para utilizar una base de datos de usuario remota.

server id Especifica el identificador de la base de datos remota.

authorization tipo_aut

Define el tipo de autorización para el inicio de sesión, PPP y el túnel. *Tipo_aut* es uno de los siguientes:

local Define el tipo de autorización para utilizar la base de datos de usuario mantenida localmente.

remote Define el tipo de autorización para utilizar una base de datos de usuario remota.

server id Especifica el identificador de la base de datos remota.

Tunnel

Utilice el mandato **tunnel** para configurar AAA para el túnel L2TP.

La Tabla 35 contiene una lista de los submandatos disponibles con el mandato **tunnel**.

<i>Tabla 35. Submandatos de Tunnel</i>	
Mandato	Función
Disable	Inhabilita la contabilidad para el túnel L2TP.
List	Muestra los parámetros de configuración de AAA para el túnel L2TP.
Set	Define los parámetros de configuración de AAA para el túnel L2TP.

Disable

Utilice el mandato **tunnel disable** para inhabilitar la contabilidad para el túnel L2TP.

Sintaxis:

tunnel disable accounting

List

Utilice el mandato **tunnel list** para visualizar la AAA para el túnel L2TP.

Sintaxis:

tunnel list all
 accounting
 authentication
 authorization
 config

Set

Utilice el mandato **tunnel set** para definir los parámetros de configuración de AAA para el túnel L2TP.

Sintaxis:

tunnel set aaa

Configuración de autenticación

accounting

authentication

authorization

aaa *tipo_aut*

Define el tipo de autenticación, autorización y contabilidad. *Tipo_aut* es uno de los siguientes:

local Define el tipo de autenticación, autorización y contabilidad para utilizar una base de datos de usuario mantenida localmente.

remote Define el tipo de autenticación, autorización y contabilidad para utilizar una base de datos de usuario remota.

server id Especifica el identificador de la base de datos remota.

accounting *tipo_aut*

Define el tipo de contabilidad. *Tipo_aut* es uno de los siguientes:

remote Define el tipo de autenticación para utilizar una base de datos de usuario remota.

server id Especifica el identificador de la base de datos remota.

authentication *tipo_aut*

Define el tipo de autenticación. *Tipo_aut* es uno de los siguientes:

local Define el tipo de autenticación para utilizar una base de datos de usuario mantenida localmente.

remote Define el tipo de autenticación para utilizar una base de datos de usuario remota.

server id Especifica el identificador de la base de datos remota.

authorization *tipo_aut*

Define el tipo de autorización. *Tipo_aut* es uno de los siguientes:

local Define el tipo de autorización para utilizar la base de datos de usuario mantenida localmente.

remote Define el tipo de autorización para utilizar una base de datos de usuario remota.

server id Especifica el identificador de la base de datos remota.

User-profiles

Utilice el mandato **user-profiles** para acceder al indicador de mandatos `User profile config`. Desde este indicador, puede acceder a los siguientes mandatos.

Tabla 36. Mandatos de configuración de perfil de usuario

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxiv.
Add	Añade un perfil de usuario de PPP.
Change	Cambia un perfil de usuario de PPP.
Delete	Suprime un perfil de usuario de PPP.
Disable	Inhabilita un perfil de usuario de PPP.
Enable	Habilita un perfil de usuario de PPP.
List	Lista la información del perfil de usuario de PPP.
Report	Genera un informe de perfil de usuario de PPP.
Reset-user	Restablece un perfil de usuario de PPP.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiv.

Add

Utilice el mandato **user profiles add** para añadir el perfil de usuario de un usuario remoto a la base de datos de usuarios de PPP local, o para dar acceso similar de túnel, a través de una red IP, al direccionador.

Sintaxis:

```
add          ppp-user
              tunnel
```

ppp-user Añade el perfil de usuario de un usuario remoto a la base de datos de usuarios de PPP local. Puede añadir hasta 500 usuarios como máximo. Añada un usuario de PPP por cada direccionador remoto o cliente DIALS que puede conectarse al dispositivo que se está configurando.

Consulte Add en el capítulo “The CONFIG Process (CONFIG - Talk 6) and Commands” del manual *Nways Multiprotocol Access Services Guía del usuario de software* para ver una descripción de la sintaxis del mandato y sus opciones.

Ejemplo:

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

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

User 'pppusr01' has been added

Ejemplo:

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

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

User 'tunusr01' has been added

tunnel Proporciona acceso similar de túnel a través de una red IP al direccionador. Entonces se autorizará al similar a iniciar sesiones PPP de túnel en el direccionador.

Consulte Add en el capítulo “Configuring the CONFIG Process” del manual *Nways Multiprotocol Access Services Guía del usuario de software* para obtener una descripción de la sintaxis del mandato y sus opciones.

Ejemplo:

```
Config> add tunnel
Enter name: []? tunne102
Enter hostname to use when connecting to this peer: []? host02
Set shared secret? (Yes, No): [No]? yes
Shared secret for tunnel authentication:
Enter again to verify:
Tunnel-Server endpoint address: [0.0.0.0]? 2.2.2.22
```

```
Tunnel name: tunne102
Endpoint: 2.2.2.22
```

Change

Utilice el mandato **change** para cambiar un perfil de usuario.

Sintaxis:

```
change      ppp-user
             tunnel
```

Delete

Utilice el mandato **delete** para suprimir un perfil de usuario.

Sintaxis:

```
delete      ppp-user
             tunnel
```

Disable

Utilice el mandato **disable** para inhabilitar un perfil de usuario.

Sintaxis:

```
disable     nombre
```

Enable

Utilice el mandato **enable** para habilitar un perfil de usuario.

Sintaxis:

```
enable     nombre
```

List

Utilice el mandato **list** para listar la información de perfil de usuario.

Sintaxis:

```
list        ppp-user
             tunnel
```

```
User profile config> list ppp-user
List (Name, Verb, User, Addr, Encr, zdump): [Verb]
  PPP user name: ppp01
    Expiry: <unlimited>
  User IP address: Interface Default
    Encryption: Not Enabled
    Status: Enabled
  Login Attempts: 0
  Login Failures: 0
  Lockout Attempts: 0
1 record displayed.
```

List Especifica cómo acceder a la información de lista.

Valores válidos: name, verb, user, addr, encr, zdump

Valor por omisión: verb

PPP user name

Lista el nombre del usuario.

Expiry Lista la fecha de caducidad.

Configuración de autenticación

User IP address

Lista la dirección IP del usuario.

Encryption

Lista si el cifrado está habilitado o inhabilitado.

Status

Lista si el estado está habilitado o inhabilitado.

Login attempts

Lista el número de veces que el usuario ha intentado iniciar la sesión.

Login failures

Lista el número de intentos fallidos de iniciar la sesión.

Lockout attempts

Lista el número de intentos de bloqueo.

Report

Utilice el mandato **report** para generar un informe de perfil de usuario de PPP.

Sintaxis:

```
report      addresses
              all
              callback
              dump
              encrypt
              name
              password
              time
              user
```

```
User profile config> report addresses
PPP user name      User IP address
-----
ppp01              Interface Default
1 record displayed.
```

```
User profile config> report all
  PPP user name: ppp01
    Expiry: <unlimited>
  User IP address: Interface Default
    Encryption: Not Enabled
    Status: Enabled
  Login Attempts: 0
  Login Failures: 0
  Lockout Attempts: 0
1 record displayed.
```

```
User profile config> report callback
PPP user name      Callback type      Phone Number
-----
ppp01
1 record displayed.
```



```
User profile config> report dump
Enter user name: []? user01
```

```
User profile config> report encrypt
PPP user name      Encryption
-----
ppp01              Not Enabled
1 record displayed.
```

```
User profile config> report name
PPP user name
-----
ppp01
1 record displayed.
```

```
User profile config> report password
PPP user name      Expiry      Grace
-----
ppp01              <unlimited>
1 record displayed.
```

```
User profile config> report time
PPP user name      Time allotted
-----
ppp01
1 record displayed.
```

```
User profile config> report user
Enter user name: []? login01
  PPP user name: login01
  Expiry: <unlimited>
  User IP address: Interface Default
  Encryption: Not Enabled
```

Reset-user

Utilice el mandato **reset-user** para restablecer un perfil de usuario.

Sintaxis:

```
reset-user      nombre
```

Configuración de autenticación

Utilización y configuración de protocolos de cifrado

Nota: El soporte del cifrado es opcional y debe añadirse a la carga del software utilizando el mandato **load add**. Consulte el mandato **load** del proceso de configuración en el manual *Nways Multiprotocol Access Services Guía del usuario de software*.

El uso del cifrado múltiple (utilizar el cifrado en la Capa de seguridad de IP y en la Capa de enlace de datos de PPP o Frame Relay) en el direccionador está restringido por la legislación de exportación del Gobierno de los Estados Unidos. Sólo está soportado en cargas de software bajo un estricto control de la exportación (cargas de software que dan soporte a RC4 con claves de 128 bits y DES triple).

El objetivo del cifrado consiste en transformar unos datos a un formato ilegible para asegurar su privacidad. Los datos **cifrados** tienen que ser descifrados para obtener los datos originales.

El 2216 da soporte a los siguientes elementos:

- El algoritmo de cifrado RC4 con claves de 40 y 128 bits para el Cifrado punto a punto de Microsoft (MPPE) en las interfaces PPP.
- El algoritmo Estándar de cifrado de datos en modalidad de encadenado de bloques de cifras (DES-CBC) con claves de 56 bits para el soporte del Protocolo de control de cifrado PPP, tal como está descrito en los RFC 1968 y 1969.
- El producto comercial Data Masking Facility (CDMF), que utiliza claves de 40 bits para el Cifrado Frame Relay. Este soporte es propietario.
- Frame Relay utiliza también triple DES y una clave de 128 bits.

Cifrado PPP utilizando el Protocolo de control de cifrado

El Protocolo de control de cifrado (ECP) se utiliza en el direccionador para negociar el uso del cifrado en los enlaces punto a punto que establecen comunicación utilizando el protocolo PPP. El Protocolo de control de cifrado proporciona un mecanismo generalizado para negociar cuáles son los algoritmos de cifrado y descifrado que se utilizarán a través de un enlace PPP. Pueden negociarse distintos algoritmos de cifrado en cada dirección del enlace PPP.

Un método de cifrado y descifrado se denomina **algoritmo de cifrado**. Los algoritmos de cifrado utilizan una clave para controlar el cifrado y el descifrado. A diferencia de la compresión, el direccionador cifra en ambas direcciones del enlace, porque el cifrado en una sola dirección representa un riesgo para la seguridad. El enlace terminará siempre que ECP no pueda negociar los algoritmos de cifrado en ambas direcciones.

Configuración del cifrado ECP para PPP

Para configurar el dispositivo para que utilice el cifrado en la capa de enlace de datos, debe realizar lo siguiente:

1. Defina las claves de cifrado para los dispositivos remotos y las interfaces PPP locales.

Defina la clave de cifrado para el dispositivo remoto, utilizando el mandato **add ppp-user** en el indicador `Config>`. Consulte el mandato **Add** en el capítulo “Configuring the CONFIG Process” del manual *Nways Multiprotocol Access Services Guía del usuario de software* para obtener una descripción de la sintaxis y las opciones del mandato.

Defina la clave de cifrado para la interfaz PPP local utilizando el mandato **enable ecp** (vea el mandato `talk 6 PPP Config>` **en el manual** *command in the Nways Multiprotocol Access Services Guía del usuario de software*).

2. Configure enlaces PPP individuales para utilizar el Protocolo de control de cifrado (ECP) mediante el mandato **enable ecp** en el indicador `PPP Config>`.
3. Habilite PAP, CHAP o SPAP.

También puede inhabilitar el cifrado, cambiar la clave de cifrado para un usuario, listar el estado de cifrado o definir el nombre que utilizará el dispositivo cuando solicite el cifrado. Para obtener información acerca de:

- Inhabilitar el cifrado, consulte el mandato `PPP Config>` **disable ecp** en el manual *Nways Multiprotocol Access Services Guía del usuario de software*.
- Cambiar la clave de cifrado y la contraseña del usuario remoto, consulte el mandato `Config>` **change ppp-user** en el manual *Nways Multiprotocol Access Services Guía del usuario de software*.
- Listar el estado de cifrado, consulte el mandato `PPP Config>` **list ecp** en el manual *Nways Multiprotocol Access Services Guía del usuario de software*.
- Definir el nombre del dispositivo, consulte el mandato `PPP Config>` **set name** en el manual *Nways Multiprotocol Access Services Guía del usuario de software*.

Supervisión del cifrado ECP para PPP

Puede supervisar los diversos valores de cifrado en las interfaces, realizando las siguientes acciones:

1. Acceda al indicador de supervisión mediante el mandato **talk 5**.
2. Seleccione la interfaz que desea supervisar mediante el mandato **network**. Este mandato le envía al indicador `PPP n>`, donde *n* representa el número de red. Consulte el apartado “Configuring and Monitoring Point-to-Point Protocol Interfaces” del manual *Nways Multiprotocol Access Services Guía del usuario de software* para obtener instrucciones acerca de la utilización del mandato **network**.

Desde este indicador, puede realizar las siguientes acciones:

- Listar el estado actual del cifrado, la negociación de cifrado más reciente, el tiempo transcurrido desde que cambió el estado de cifrado y los algoritmos utilizados por los cifradores. (Consulte el mandato **list control ecp** en el manual *Nways Multiprotocol Access Services Guía del usuario de software*.)

- Listar los paquetes de control de cifrado recibidos y transmitidos en la interfaz. (Consulte el mandato **list ecp** en el manual *Nways Multiprotocol Access Services Guía del usuario de software*.)
- Listar los paquetes de datos cifrados transmitidos o recibidos en la interfaz. (Consulte el mandato **list edp** en el manual *Nways Multiprotocol Access Services Guía del usuario de software*.)

Cifrado punto a punto de Microsoft (MPPE)

El Cifrado punto a punto de Microsoft (MPPE) proporciona, a las estaciones de trabajo Windows conectadas de forma remota que son conocidas como clientes DUN (Redes de marcación de Microsoft), una manera de cifrar los datos que se transmiten a través de un enlace PPP entre ellos y el 2216. MPPE también puede utilizarse para cifrar los datos que se transmiten a través de un enlace PPP de direccionador a direccionador. MPPE siempre se negocia en ambas direcciones.

MPPE utiliza los algoritmos de clave secreta para realizar el cifrado. En los algoritmos de clave secreta, se utiliza la misma clave para el cifrado y el descifrado. El usuario no configura esta clave, sino que se genera durante el proceso de negociación de MPPE entre las estaciones de trabajo remitente y destinataria. Para utilizar MPPE, debe configurar el protocolo de autenticación MS-CHAP (Microsoft Challenge/Handshake Authentication Protocol).

Si la interfaz PPP se autentica con MS-CHAP, el direccionador entra en una “modalidad Microsoft”, en la que sólo negociará MPPC si la compresión está habilitada y sólo negociará MPPE si el cifrado está habilitado. En la “modalidad Microsoft”, el direccionador pasa por alto la lista de prioridades de los algoritmos de compresión e inhabilita la negociación de ECP.

Configuración de MPPE

Para configurar MPPE, debe realizar los siguientes pasos para cada interfaz:

1. Configure MS-CHAP. En el manual *Nways Multiprotocol Access Services Guía del usuario de software*, consulte “Microsoft PPP CHAP Authentication (MS-CHAP)” y “Configuring and Monitoring Point-to-Point Protocol Interfaces” para obtener información acerca de la utilización y la configuración de MS-CHAP.
2. Si configura una conexión de direccionador a direccionador, defina el nombre de la interfaz PPP local mediante el mandato **set name** (consulte el mandato PPP Config> **set name** en el manual *Nways Multiprotocol Access Services Guía del usuario de software*).
3. Si desea realizar la compresión de datos, habilite MPPC utilizando el mandato talk 6 **enable ccp** en el indicador Config>. MPPE no requiere la compresión de datos.
4. Habilite MPPE. Utilice el mandato **enable mppe** en el indicador PPP Config> (consulte el mandato PPP Config> **enable** en el manual *Nways Multiprotocol Access Services Guía del usuario de software*).
5. Reinicie el direccionador para activar la configuración.

También puede inhabilitar MPPE y listar las opciones de MPPE.

- Utilice el mandato talk 6 **disable mppe** en el indicador PPP Config> para inhabilitar MPPE.
- Utilice el mandato talk 6 **list ccp** en el indicador PPP Config> para listar las opciones de MPPE que se han configurado.

Supervisión de MPPE

Haga que aparezca el indicador PPP>, tal como se describe en “Supervisión del cifrado ECP para PPP” en la página 280. Utilice el mandato **list mppe** para ver las estadísticas de datos de MPPE y el mandato **list control ccp** para ver el estado de MPPE. Se visualizan unos ejemplos de las salidas de estos mandatos en el apartado “Configuring and Monitoring Point-to-Point Protocol Interfaces” del manual *Nways Multiprotocol Access Services Guía del usuario de software*.

Configuración del cifrado en interfaces Frame Relay

Nota: Frame Relay utiliza un esquema de cifrado propietario.

El cifrado de datos está soportado en todas las interfaces en las que ha habilitado el cifrado. Puede configurar circuitos individuales en una interfaz habilitada para el cifrado para realizar el cifrado o no, como desee.

Para configurar el dispositivo con el fin de utilizar el cifrado en enlaces Frame Relay:

1. Acceda al indicador de configuración de Frame Relay utilizando el mandato **talk 6**.
2. Seleccione la interfaz Frame Relay que desea que tenga capacidad de cifrado, utilizando el mandato **net #**
3. Habilite el cifrado en la interfaz Frame Relay utilizando el mandato **enable encryption**. Consulte los mandatos de configuración de Frame Relay en el manual *Nways Multiprotocol Access Services Guía del usuario de software*.
4. Añada los circuitos virtuales permanentes con capacidad de cifrado y defina la clave de cifrado para cada PVC utilizando el mandato **add permanent-virtual-circuit**. Consulte los mandatos de configuración de Frame Relay en el manual *Nways Multiprotocol Access Services Guía del usuario de software*.
5. Repita los pasos 1 a 4 para cada interfaz con capacidad de cifrado que está configurando.

Nota: Si está habilitado el cifrado para un circuito virtual permanente FR, los datos pasarán por el circuito a menos que el cifrado se negocie satisfactoriamente con el dispositivo en el otro extremo del circuito virtual. El cifrado no está soportado para circuitos huérfanos, dado que debe configurar el PVC para entrar la clave de cifrado.

También puede inhabilitar el cifrado para una interfaz, cambiar los valores de cifrado para un PVC o listar el estado de cifrado. Para obtener información acerca de

- Inhabilitar el cifrado en una interfaz, consulte el mandato de Configuración de Frame Relay **disable encryption** en el manual *Nways Multiprotocol Access Services Guía del usuario de software*.

- Cambiar los valores de cifrado para un PVC, consulte el mandato de Configuración de Frame Relay **change permanent-virtual-circuit** en el manual *Nways Multiprotocol Access Services Guía del usuario de software*.
- Listar el estado de cifrado, consulte los mandatos de Configuración de Frame Relay **list all**, **list lmi** y **list permanent-virtual-circuit** en el manual *Nways Multiprotocol Access Services Guía del usuario de software*.

Supervisión del cifrado en interfaces Frame Relay

Puede supervisar los diversos valores de cifrado en las interfaces, realizando las siguientes acciones:

1. Acceda al indicador de supervisión mediante el mandato **talk 5**.
2. Seleccione la interfaz que desea supervisar mediante el mandato **network #**. Este mandato le envía al indicador FR x>.

En este indicador, puede listar el estado de cifrado actual para una interfaz, un PVC o un circuito. Consulte el mandato de Supervisión de Frame Relay **list** en el manual *Nways Multiprotocol Access Services Guía del usuario de software*.

Configuración y supervisión de la Calidad de los servicios (QoS)

Este capítulo describe la configuración y los mandatos operativos de la Calidad de los servicios (QoS) para las interfaces LAN y ELAN en el dispositivo. Contiene las secciones siguientes:

- “Visión general de la Calidad de los servicios”
- “Parámetros de configuración de QoS” en la página 286
- “Acceso al indicador de configuración de QoS” en la página 291
- “Mandatos de Calidad de los servicios” en la página 292
- “Mandatos de configuración de QoS de LE Client” en la página 292
- “Mandatos de configuración de QoS de la interfaz ATM” en la página 297
- “Acceso a los mandatos de supervisión de QoS” en la página 300
- “Mandatos de supervisión de Calidad de los servicios” en la página 300
- “Mandatos de supervisión de QoS de LE Client” en la página 301

Visión general de la Calidad de los servicios

La característica QoS aumenta las ventajas de las posibilidades de ATM QoS para las LAN Emulation Data Direct VCC. Se hace referencia a este soporte como “QoS configurable para Emulación de LAN”. Los atributos clave y las ventajas de esta característica son los siguientes:

- Un LE Client utiliza los parámetros configurados de QoS para sus Data Direct VCC.
- Se pueden configurar parámetros de QoS para:
 - LE Client
 - Interfaz ATM
- El conjunto de los parámetros de QoS configurados son para su utilización con la señalización ATM Forum UNI 3.0/3.1. Los parámetros incluyen los valores deseados de Velocidad mayor de célula, Velocidad sostenida de célula, Clase de QoS y Tamaño máximo de ráfaga.
- El Ancho de banda máximo reservado por VCC puede configurarse para proteger un LE Client de la aceptación/establecimiento de las VCC a cuyos parámetros de tráfico no se puede dar soporte.
- El mecanismo de Negociación de QoS permite que los LE Clients participantes tengan en cuenta mutuamente sus parámetros de QoS. Se configura una VCC data-direct utilizando los parámetros negociados.

Ventajas de QoS

- La utilización de QoS para el LE Client, Interfaz ATM o LAN emulada, proporciona las siguientes ventajas para las VCC LANE Data Direct.
 - Un LE Client se puede configurar con QoS si los QoS que requiere el cliente son distintos de los que requieren otros clientes de la ELAN. Por ejemplo, si un LE Client sirve a un servidor de archivos, puede que el usuario desee configurar los parámetros adecuados de QoS para todo el tráfico que va al servidor de archivos y que procede de él.

Configuración de la Calidad de los servicios (QoS)

- Una LAN emulada se puede configurar con QoS si el usuario desea proporcionar QoS para todo el tráfico en esa ELAN. Por ejemplo, se puede dar prioridad a una ELAN que transporte tráfico de SNA configurando los parámetros de QoS para esa ELAN.
- Una Interfaz ATM se puede configurar con QoS si un usuario desea que todos los LE Clients en esa Interfaz ATM utilicen el mismo conjunto de parámetros. Por ejemplo, si una Interfaz ATM está conectada a 25 Mbps, el usuario puede configurar los parámetros adecuados que sean distintos de los que corresponden a una interfaz a 155 Mbps.

Parámetros de configuración de QoS

Esta sección describe nueve parámetros que se utilizan para la configuración de QoS. Los seis parámetros siguientes pueden configurarse para un LE Client Interfaz AT y una LAN emulada:

1. `max-reserved-bandwidth`
2. `traffic-type`
3. `peak-cell-rate`
4. `sustained-cell-rate`
5. `max-burst-size`
6. `qos-class`

Los dos parámetros siguientes pueden configurarse para una LAN emulada y un LE Client:

1. `validate-pcr-of-best-effort-vccs`
2. `negotiate-qos`

El parámetro `accept-qos-parms-from-lecs` sólo se puede configurar para un LE Client.

Los seis primeros parámetros controlan las características de tráfico de las VCC Data Direct establecidas por el LE Client, mientras que el primer parámetro se aplica también a las llamadas recibidas por el LE Client. Las siguientes características están asociadas a todas las VCC Data Direct establecidas por el LE Client:

- El ancho de banda no está reservado para el tráfico de mejor esfuerzo (best-effort).
- Los parámetros de tráfico se aplican en ambos sentidos.
- Cuando se rechaza una conexión de ancho de banda reservado debido a los parámetros de tráfico o la clase de QoS, se reintenta la llamada como una conexión de mejor esfuerzo con la velocidad mayor de célula configurada (hace que se utilicen códigos en los mensajes `release` o `release-complete` para determinar la razón de que se haya liberado una VCC).
- Cuando se rechaza una conexión de mejor esfuerzo debido a la Velocidad mayor de célula (PCR), se puede reintentar la llamada automáticamente con una PCR más baja. Los reintentos se realizan en las siguientes condiciones:
 1. Si la PCR rechazada es mayor que 100 Mbps, la llamada se reintenta con una PCR de 100 Mbps.

2. En caso contrario contrario, si la PCR rechazada es mayor que 25 Mbps, la llamada se reintenta con una PCR de 25 Mbps.

Ancho de banda máximo reservado (max-reserved-bandwidth)

El ancho de banda máximo reservado que es aceptable para una VCC Data Direct. Este parámetro se aplica a las llamadas de VCC Data Direct recibidas por el LE Client y las llamadas de VCC Data Direct hechas por el LE Client. Para las llamadas entrantes, este parámetro define la SCR máxima aceptable para una VCC Data Direct. Si no se especifica la SCR en la llamada entrante, este parámetro define la PCR máxima aceptable para una VCC Data Direct con el ancho de banda reservado.

Se liberarán las llamadas recibidas con parámetros de tráfico que especifiquen velocidades mayores. Si se especifica SCR en la llamada entrante, la llamada no se rechazará debido a la PCR o al Tamaño máximo de ráfaga. La restricción impuesta por este parámetro no es aplicable a las conexiones best_effort (de mejor esfuerzo). Para las llamadas salientes, este parámetro define un límite superior de la cantidad de ancho de banda reservado que puede solicitarse para una VCC Data Direct. Por consiguiente, los parámetros traffic-type y sustained-cell-rate dependen de este parámetro.

Valores válidos:

Un entero en el rango de 0 a la velocidad de línea del dispositivo ATM en Kbps

Valor por omisión:

0

Tipo de tráfico (traffic-type)

Tipo de tráfico deseado para las VCC Data Direct. Si no se negocian los parámetros de QoS, este parámetro especifica el tipo de llamadas hechas por el LE Client. De lo contrario, si se negocian los parámetros de QoS, este parámetro especifica el tipo deseado de las características de tráfico para las VCC Data Direct. Cuando se negocian los parámetros de QoS, si el LEC de origen o de destino desea una conexión de ancho de banda reservado y ambos LEC dan soporte a conexiones de ancho de banda (es decir, si max-reserved-bandwidth > 0), se realizará un intento de establecer una VCC Data Direct de ancho de banda reservado entre ambos LEC. De lo contrario, la VCC Data Direct VCC será una conexión best_effort. Dependencias: max-reserved-bandwidth

Valores válidos:

best_effort o reserved_bandwidth

Valor por omisión:

best_effort

Velocidad mayor de célula (peak-cell-rate)

Velocidad mayor de célula deseada para las VCC Data Direct. Si no se negocian los parámetros de QoS, este parámetro especifica el parámetro de tráfico de PCR para las llamadas de VCC Data Direct hechas por el LE Client. De lo contrario, si se negocian los parámetros de QoS, este parámetro especifica el parámetro de tráfico de PCR para las VCC Data Direct. Se utiliza el valor mínimo de las PCR deseadas de los dos LEC para las VCC de mejor esfuerzo negociadas.

Configuración de la Calidad de los servicios (QoS)

Cuando se negocia una VCC de ancho de banda reservado y sólo uno de los LE Clients solicita una conexión de ancho de banda reservado, se utiliza la PCR deseada de ese LEC para la VCC Data Direct, sujeta al límite superior impuesto por la velocidad de línea del dispositivo ATM local. Si ambos LEC solicitan una conexión de ancho de banda reservado, se utiliza el valor máximo de las PCR deseadas de los LE Clients para la VCC Data Direct, sujeto al límite superior impuesto por la velocidad de línea del dispositivo ATM local.

Valores válidos:

Un valor entero en el rango de 0 a la velocidad de línea del dispositivo ATM en Kbps

Valor por omisión:

Velocidad de línea del Dispositivo ATM de LEC en Kbps.

Velocidad sostenida de célula (sustained-cell-rate)

Velocidad sostenida de célula deseada para las VCC Data Direct. Si no se negocian los parámetros de QoS, este parámetro especifica el parámetro de tráfico de SCR para las llamadas de VCC Data Direct hechas por el LE Client. De lo contrario, si se negocian los parámetros de QoS, este parámetro especifica el parámetro de tráfico de SCR para las VCC Data Direct.

Cuando se negocia una VCC de ancho de banda reservado y sólo uno de los LE Clients solicita una conexión de ancho de banda reservado, se utiliza la SCR deseada de ese LEC para la VCC Data Direct (sujeta al límite superior impuesto por la velocidad de línea del otro LEC). Si ambos LEC solicitan una conexión de ancho de banda reservado, se utiliza el valor máximo de las SCR deseadas de los LE Clients para la VCC Data Direct (sujeto al límite superior impuesto por los parámetros max-reserved-bandwidth de ambos LEC). En cualquier caso (haya negociación o no), si la SCR que debe señalarse es igual a la PCR que tiene que señalarse, la llamada se señala sólo con PCR.

Dependencias: max-reserved-bandwidth, traffic-type y peak-cell-rate. Este parámetro sólo es aplicable cuando el valor de traffic-type es reserved_bandwidth.

Valores válidos:

Un valor entero en el rango de 0 al mínimo de max-reserved-bandwidth y peak-cell-rate, especificado en Kbps

Valor por omisión

Ninguno

Tamaño máximo de ráfaga (max-burst-size)

El tamaño máximo de ráfaga deseado para las VCC Data Direct. Si no se negocian los parámetros de QoS, este parámetro especifica el parámetro de tráfico de Tamaño máximo de ráfaga para las llamadas de VCC Data Direct hechas por el LE Client. De lo contrario, si se negocian los parámetros de QoS, este parámetro especifica el parámetro de tráfico de Tamaño máximo de ráfaga para las VCC Data Direct.

Cuando se negocia una VCC de ancho de banda reservado y sólo uno de los LE Clients solicita una conexión de ancho de banda reservado, se utiliza el Tamaño máximo de ráfaga deseado de ese LEC para la VCC Data Direct. Si ambos LEC solicitan una conexión de ancho de banda reservado, se utiliza el valor máximo de

los Tamaños máximos de ráfaga deseados de los LE Clients para la VCC Data Direct.

En cualquier caso (haya una negociación o no), el Tamaño máximo de ráfaga sólo se señala cuando se señala la SCR. Aunque este parámetro se expresa en unidades de células, se configura como un múltiplo entero del Tamaño máximo de trama de datos (especificado en el parámetro C3 de LEC) con un límite inferior igual a 1.

Dependencias: este parámetro sólo es aplicable cuando el valor de traffic-type es reserved_bandwidth.

Valores válidos:

Un número entero de tramas; debe ser mayor que 0

Valor por omisión:

1 trama

Clase de QoS (qos-class)

Clase de QoS deseada para las llamadas de ancho de banda reservadas. Si no se negocian los parámetros de QoS, este parámetro especifica la Clase de QoS que debe utilizarse para las llamadas de VCC Data Direct de ancho de banda reservado hechas por el LE Client. De lo contrario, si se negocian los parámetros de QoS, este parámetro especifica la Clase de QoS que se desea para las VCC Data Direct. Siempre se utiliza una Clase de QoS no especificada en las llamadas de mejor esfuerzo. Las Clases de QoS especificadas definen valores objetos para el rendimiento de ATM. Las Clases de QoS especificadas definen valores objetivos para los parámetros de rendimiento de ATM, tales como la proporción de pérdida de células y el retardo de transferencia de células.

La Especificación de UNI indica que:

Clase 1 de QoS especificada

debe dar un rendimiento comparable con el rendimiento actual de línea privada digital.

Clase 2 de QoS especificada

pensada para el vídeo y audio en paquetes, en aplicaciones de teleconferencia y multimedia.

Clase 3 de QoS especificada

pensada para la interoperación de los protocolos orientados a la conexión, como Frame Relay.

Clase 4 de QoS especificada

pensada para la interoperación de los protocolos sin conexión, como IP o SMDS.

Los LEC deben poder aceptar llamadas con cualquiera de las Clases de QoS anteriores. Cuando se negocian los parámetros de QoS, se comparan las Clases de QoS configuradas de los dos LEC y se utiliza la Clase de QoS con los requisitos más restrictivos.

Valores válidos:

0: para la Clase de QoS no especificada

1: para la Clase 1 de QoS especificada

Configuración de la Calidad de los servicios (QoS)

2: para la Clase 2 de QoS especificada

3: para la Clase 3 de QoS especificada

4: para la Clase 4 de QoS especificada

Valor por omisión:

0 (Clase de QoS no especificada)

Validar PCR de VCC de mejor esfuerzo (validate-pcr-of-best-effort-vccs)

Validar la Velocidad mayor de célula de las VCC de mejor esfuerzo. Cuando el valor sea FALSE, las VCC de mejor esfuerzo se aceptarán sin tener en cuenta la PCR de avance señalizada. Cuando el valor sea TRUE, las VCC de mejor esfuerzo se rechazarán si la PCR de reenvío señalizada sobrepasa la velocidad de línea del dispositivo ATM de LE Client. Las llamadas no se rechazarán, debido a la PCR de retroceso. Se respetará la PCR de retroceso señalizada, si no sobrepasa la velocidad de línea; de lo contrario, las transmisiones al llamante a la velocidad de línea.

Notas:

1. Aceptar las VCC de mejor esfuerzo con las PCR de avance que sobrepasan la velocidad de línea, puede causar un bajo rendimiento debido a un exceso de retransmisiones; no obstante, rechazar estas VCC puede provocar problemas de interoperabilidad.
2. El valor yes es útil cuando los llamantes hacen un reintento con una PCR menor, después de una llamada rechazada a causa de una velocidad de célula no disponible.

Valores válidos:

yes, no

Valor por omisión:

no

Negociar QoS (negotiate-qos)

Habilitar la negociación de parámetros de QoS para las VCC Data Direct. Sólo debe habilitarse este parámetro cuando se establezca conexión con un IBM MSS LES. Cuando el valor de este parámetro sea yes, el LE Client incluirá un IBM Traffic Parameter TLV en las tramas LE_JOIN_REQUEST y LE_ARP_RESPONSE enviadas al LES. Este TLV incluirá los valores de max-reserved-bandwidth, traffic-type, peak-cell-rate, sustained-cell-rate, max-burst-size y qos-class. También se puede incluir un IBM Traffic Parameter TLV en un LE_ARP_RESPONSE devuelto al LE Client por el LES.

Si no hay ningún TLV en un LE_ARP_RESPONSE recibido por el LE Client, deben utilizarse los parámetros de la configuración local para configurar la VCC Data Direct. Si se incluye un TLV en un LE_ARP_RESPONSE, el LE Client debe comparar el contenido del TLV con los valores locales correspondientes para determinar el conjunto de parámetros “negociados” o “mejores” que sea aceptable para ambas partes antes de señalar la VCC Data Direct.

Valores válidos:

yes, no

Valor por omisión:

no

Aceptar parámetros QoS de LECS (accept-qos-params-from-lecs)

Este parámetro proporciona la capacidad de configurar un LE Client para aceptar o rechazar parámetros de QoS de un LECS. Cuando este parámetro es yes, el LE Client debe utilizar los parámetros de QoS obtenidos de los LE Clients en las tramas LE_CONFIGURE_RESPONSE, es decir, los parámetros de QoS de los LE Clients prevalecen sobre los parámetros de QoS configurados localmente. Si este parámetro es no, el LE Client pasará por alto cualquier parámetro de QoS recibido en una trama LE_CONFIGURE_RESPONSE de los LE Clients.

Valores válidos:

yes, no

Valor por omisión:

no

Acceso al indicador de configuración de QoS

Utilice el mandato **feature** del proceso CONFIG para acceder a los mandatos de configuración de Calidad de los servicios. Entre **feature** seguido del número de característica (6) o el nombre corto (QoS). Por ejemplo:

```
Config> feature qos
Calidad de los servicios
- Configuración
QoS Config>
```

Una vez que haya accedido al indicador QoS Config>, puede configurar la Calidad de los servicios (QoS) de un LE Client, o una interfaz ATM. Para regresar al indicador Config> en cualquier momento, entre el mandato **exit** en el indicador QoS Config>.

Por otra parte, puede configurar parámetros de QoS para un LE Client o una interfaz ATM accediendo a las entidades de la manera siguiente:

- LE Client

1. En el indicador Config>, entre el mandato **network** y el número de interfaz de LE Client.
2. En el indicador LE Client configuration>, entre **qos-configuration**.

Ejemplo:

```
config> network 3
Token Ring Forum Compliant LEC Config> qos-configuration
LEC QoS Config>
```

- Interfaz ATM

1. En el indicador Config>, entre el mandato **network** y el número de interfaz ATM para acceder al indicador ATM Config>.
2. Entre el parámetro **interface** para acceder al indicador ATM Interface Config>.
3. En el indicador ATM InterfaceConfig>, entre **qos-configuration**.

Ejemplo:

Configuración de la Calidad de los servicios (QoS)

```
config> network 0
ATM Config> interface
ATM Interface Config> qos-configuration
ATM-I/F 0 QoS>
```

Mandatos de Calidad de los servicios

Esta sección resume los mandatos de configuración de QoS. Utilice los siguientes mandatos para configurar la Calidad de los servicios. Entre los mandatos en el indicador QoS Config>.

Tabla 37. Resumen de los mandatos de configuración de la Calidad de los servicios (QoS)

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxiv.
le-client	Le permite acceder al indicador LE Client QoS configuration > para el LE Client seleccionado.
atm-interface	Le permite acceder al indicador ATM Interface QoS configuration> para la interfaz ATM seleccionada.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiv.

Mandatos de configuración de QoS de LE Client

En esta sección se resumen y se explican los mandatos de configuración de QoS para un LE Client específico.

Utilice los mandatos siguientes en el indicador LEC QoS config>.

Tabla 38. Resumen de los mandatos de configuración de la Calidad de los servicios (QoS) de LE Client

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxiv.
List	Lista la configuración de QoS actual del LE Client.
Set	Define los parámetros de QoS del LE Client.
Remove	Elimina la configuración de QoS del LE Client.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiv.

List

Utilice el mandato **list** para listar la configuración de este LE Client. Los parámetros QoS sólo se listan si al menos uno de ellos se ha configurado de manera específica (vea el Ejemplo 1). De lo contrario, no se listará ningún parámetro (vea el Ejemplo 2).

Sintaxis:

list

Ejemplo 1:

LEC QoS Config> **list**

```

      LE Client QoS Configuration for Data Direct VCCs
      =====
      (ATM interface number = 0,  LEC interface number = 3)

      Maximum Reserved Bandwidth for a Data-Direct VCC = 10000 Kbps
      Data-Direct VCC Type ..... = Best-Effort
      Data-Direct VCC Peak Cell Rate ..... = 155000 Kbps
      Data-Direct VCC Sustained Cell Rate ..... = 155000 Kbps
      Desired QoS Class of Reserved Connections ..... = 0
      Max Burst Size of Reserved Connections ..... = 0 frames

      Validate Peak Rate of Best-Effort connections .. = No
      Enable QoS Parameter Negotiation ..... = Yes
      Accept QoS Parameters from LECS ..... = Yes
    
```

LEC QoS Config>

Ejemplo 2:

LEC QoS Config> **list**

```

      QoS has not been configured for this LEC.
      Please use the SET option to configure QoS.
    
```

LEC QoS Config>

Set

Utilice el mandato **set** para especificar los parámetros de QoS de LE Client.

Sintaxis:

```

set          accept-qos-parms-from-lecs
              all-default-values
              max-burst-size
              max-reserved-bandwidth
              negotiate-qos
              peak-cell-rate
              qos-class
              sustained-cell-rate
              traffic-type
              validate-pcr-of-best-effort-vccs
    
```

accept-qos-parms-from-lecs

Utilice esta opción para habilitar/inhabilitar el LE Client para aceptar/rechazar los parámetros de QoS recibidos de un LECS como

Configuración de la Calidad de los servicios (QoS)

TLV. Consulte “Aceptar parámetros QoS de LECS (accept-qos-params-from-lecs)” en la página 291 para ver una descripción más detallada de este parámetro.

Valores válidos:

yes, no

Valor por omisión:

yes

Ejemplo:

```
LEC QoS Config> se acc y
LEC QoS Config>
```

all-default-values

Utilice esta opción para definir los parámetros de QoS con los valores por omisión. En el ejemplo siguiente se listan también los valores por omisión.

Ejemplo:

```
LEC QoS Config> set all-default-values
Failed to locate existing QoS configuration record!
Using a new set of default values ...
Initializing all parameters to default values
LEC QoS Config> list

      LE Client QoS Configuration for Data Direct VCCs
      =====
      (ATM interface number = 0,  LEC interface number = 3)

      Maximum Reserved Bandwidth for a Data-Direct VCC = 0 Kbps
      Data-Direct VCC Type ..... = Best-Effort
      Data-Direct VCC Peak Cell Rate ..... = 155000 Kbps
      Data-Direct VCC Sustained Cell Rate ..... = 155000 Kbps
      Desired QoS Class of Reserved Connections ..... = 0
      Max Burst Size of Reserved Connections ..... = 0 frames

      Validate Peak Rate of Best-Effort connections .. = No
      Enable QoS Parameter Negotiation ..... = No
      Accept QoS Parameters from LECS ..... = Yes

LEC QoS Config>
```

max-burst-size

Define el tamaño máximo de ráfaga deseado en las tramas. Consulte “Tamaño máximo de ráfaga (max-burst-size)” en la página 288 para ver una descripción más detallada de este parámetro.

Valores válidos:

Un número entero de tramas; debe ser mayor que 0

Valor por omisión:

1 trama

Ejemplo:

```
LEC QoS Config> se ma
Maximum Burst Size in Kbps [1]? 10000
LEC QoS Config>
```

max-reserved-bandwidth

Utilice esta opción para definir el ancho de banda máximo reservado que está permitido por VCC Data Direct. Consulte “Ancho de banda máximo reservado (max-reserved-bandwidth)” en la página 287 para ver una descripción más detallada de este parámetro.

Valores válidos: Un entero en el rango de 0 a la velocidad de línea del dispositivo ATM en Kbps

Valor por omisión: 0

Ejemplo:

```
LEC QoS Config> set max-reserved-bandwidth
Maximum reserved bandwidth acceptable for a data-direct VCC (in Kbps) [0]? 20000
LEC QoS Config>
```

negotiate-qos

Utilice esta opción para habilitar/inhabilitar la partición del LE Client en la negociación de QoS. Consulte “Negociar QoS (negotiate-qos)” en la página 290 para ver una descripción más detallada de este parámetro.

Valores válidos:

yes, no

Valor por omisión:

no

Ejemplo:

```
LEC QoS Config> se neg y
LEC QoS Config>
```

peak-cell-rate

Define la velocidad mayor de célula deseada para Data Direct. Consulte “Velocidad mayor de célula (peak-cell-rate)” en la página 287 para ver una descripción más detallada de este parámetro.

Valores válidos:

Un valor entero en el rango de 0 a la velocidad de línea del dispositivo ATM en Kbps

Valor por omisión:

Velocidad de línea del Dispositivo ATM de LEC en Kbps.

Ejemplo:

```
LEC QoS Config> set peak-cell-rate
Data-Direct VCC Peak Cell Rate in Kbps [1]? 25000
LEC QoS Config>
```

qos-class

Define la Clase de QoS deseada para las VCC Data Direct. Consulte “Clase de QoS (qos-class)” en la página 289 para ver una descripción más detallada de este parámetro.

Valores válidos:

0: para la Clase de QoS no especificada

1: para la Clase 1 de QoS especificada

2: para la Clase 2 de QoS especificada

3: para la Clase 3 de QoS especificada

4: para la Clase 4 de QoS especificada

Valor por omisión:

0 (Clase de QoS no especificada)

Ejemplo:

```
LEC QoS Config> se qos
Desired QoS Class for Data Direct VCCs [0]? 1
LEC QoS Config>
```

sustained-cell-rate

Define la velocidad sostenida de célula deseada para las VCC Data Direct. Consulte “Velocidad sostenida de célula (sustained-cell-rate)” en

Configuración de la Calidad de los servicios (QoS)

la página 288 para ver una descripción más detallada de este parámetro.

Valores válidos:

Un valor entero en el rango de 0 al mínimo de max-reserved-bandwidth y peak-cell-rate, especificado en Kbps

Valor por omisión

Ninguno

Ejemplo:

```
LEC QoS Config> se sus
Data-Direct VCC Sustained Cell Rate in Kbps [1]? 10000
LEC QoS Config>
```

traffic-type

Define el tráfico deseado para las VCC Data Direct. Consulte “Tipo de tráfico (traffic-type)” en la página 287 para ver una descripción más detallada de este parámetro.

Valores válidos:

best effort o reserved bandwidth

Valor por omisión:

best effort

Ejemplo:

```
LEC QoS Config>set traffic-type
Choose from:
(0): Best-Effort
(1): Reserved-Bandwidth
Data Direct VCC Type [0]? 1
Note: Peak Cell Rate has been reset to 1
      Sustained Cell Rate has been reset to 1
      Max Reserved Bandwidth has been reset to 1
      Please configure appropriate values.
LEC QoS Config>
```

validate-pcr-of-best-effort-vccs

Utilice esta opción para habilitar/inhabilitar la validación del parámetro de tráfico de Velocidad mayor de célula de las llamadas de VCC Data Direct recibidas por este LE Client. Consulte “Validar PCR de VCC de mejor esfuerzo (validate-pcr-of-best-effort-vccs)” en la página 290 para ver una descripción más detallada de este parámetro.

Valores válidos:

yes, no

Valor por omisión:

no

Ejemplo:

```
LEC QoS Config> se val y
LEC QoS Config>
```

Remove

Utilice el mandato **remove** para eliminar la configuración de QoS de este LE Client.

Sintaxis:

remove

Ejemplo:

```
LEC QoS Config> remove
WARNING: This option deletes the QoS configuration.
         To re-configure use any of the SET options.
Should the LEC QoS configuration be deleted? [No]: yes
Deleted QoS configuration successfully
LEC QoS Config>
```

Mandatos de configuración de QoS de la interfaz ATM

<i>Tabla 39. Resumen de los mandatos de configuración de la Calidad de los servicios (QoS) de LE Client</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 el apartado "Cómo obtener ayuda" en la página xxxiv.
List	Lista la configuración de QoS actual de la interfaz ATM.
Set	Define los parámetros de QoS de interfaz ATM.
Remove	Elimina la configuración de QoS de la interfaz ATM.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página xxxiv.

List

Utilice el mandato **list** para listar la configuración de QoS de esta interfaz ATM. Los parámetros sólo se listan si se ha configurado al menos uno de ellos (vea el ejemplo siguiente). De lo contrario, no se listará ningún parámetro.

Sintaxis:

list

Ejemplo:

```
ATM-I/F 0 QoS> list

      ATM Interface Quality of Service' Configuration
      =====
      (ATM interface number = 0 )

      Maximum Reserved Bandwidth for a VCC = 15000 Kbps
      VCC Type ..... = RESERVED-BANDWIDTH
      Peak Cell Rate ..... = 20000 Kbps
      Sustained Cell Rate ..... = 5000 Kbps
      QoS Class ..... = 4
      Maximum Burst Size ..... = 5 frames
ATM-I/F 0 QoS>
```

Set

Utilice el mandato **set** para especificar los parámetros de QoS de la interfaz ATM.

Sintaxis:

```
set          max-burst-size
              max-reserved-bandwidth
              peak-cell-rate
```

Configuración de la Calidad de los servicios (QoS)

qos-class

sustained-cell-rate

traffic-type

max-burst-size

Define el tamaño máximo de ráfaga deseado en las tramas. Consulte “Tamaño máximo de ráfaga (max-burst-size)” en la página 288 para ver una descripción más detallada de este parámetro.

Valores válidos:

Un número entero de tramas; debe ser mayor que 0

Valor por omisión:

1 trama

Ejemplo:

```
ATM-I/F 0 QoS Config> se ma
Maximum Burst Size in Kbps [1]? 10000
ATM-I/F 0 QoS Config>
```

max-reserved-bandwidth

Utilice esta opción para definir el ancho de banda máximo reservado que está permitido para cada VCC Data Direct. Consulte “Ancho de banda máximo reservado (max-reserved-bandwidth)” en la página 287 para ver una descripción más detallada de este parámetro.

Valores válidos:

Un entero en el rango de 0 a la velocidad de línea del dispositivo ATM en Kbps

Valor por omisión:

0

Ejemplo:

```
ATM-I/F 0 QoS> se max-reserved-bandwidth
Maximum reserved bandwidth acceptable for a data-direct VCC (in Kbps) [0]?
15000
ATM-I/F 0 QoS>
```

peak-cell-rate

Define la velocidad mayor de célula deseada para las VCC Data Direct. Consulte “Velocidad mayor de célula (peak-cell-rate)” en la página 287 para ver una descripción más detallada de este parámetro.

Valores válidos:

Un valor entero en el rango de 0 a la velocidad de línea del dispositivo ATM en Kbps

Valor por omisión:

Velocidad de línea del Dispositivo ATM de LEC en Kbps.

Ejemplo:

```
ATM-I/F 0 QoS Config> set peak-cell-rate
Data-Direct VCC Peak Cell Rate in Kbps [1]? 25000
ATM-I/F 0 QoS Config>
```

qos-class

Define la Clase de QoS deseada para las VCC Data Direct. Consulte “Clase de QoS (qos-class)” en la página 289 para ver una descripción más detallada de este parámetro.

Valores válidos:

- 0: para la Clase de QoS no especificada
- 1: para la Clase 1 de QoS especificada
- 2: para la Clase 2 de QoS especificada
- 3: para la Clase 3 de QoS especificada
- 4: para la Clase 4 de QoS especificada

Valor por omisión:

0 (Clase de QoS no especificada)

Ejemplo:

```
ATM-I/F 0 QoS Config> se qos
Desired QoS Class for Data Direct VCCs [0]? 1
ATM-I/F 0 QoS Config>
```

sustained-cell-rate

Define la velocidad sostenida de célula deseada para las VCC Data Direct. Consulte “Velocidad sostenida de célula (sustained-cell-rate)” en la página 288 para ver una descripción más detallada de este parámetro.

Valores válidos:

Un valor entero en el rango de 0 al mínimo de max-reserved-bandwidth y peak-cell-rate, especificado en Kbps

Valor por omisión

Ninguno

Ejemplo:

```
ATM-I/F 0 QoS Config> se sus
Data-Direct VCC Sustained Cell Rate in Kbps [1]? 10000
ATM-I/F 0 QoS Config>
```

traffic-type

Define el tráfico deseado para las VCC Data Direct. Consulte “Tipo de tráfico (traffic-type)” en la página 287 para ver una descripción más detallada de este parámetro.

Valores válidos:

best_effort o reserved_bandwidth

Valor por omisión:

best_effort.

Ejemplo:

```
ATM-I/F 0 QoS> set traffic-type
Choose from:
(0): Best-Effort
(1): Reserved Bandwidth
Traffic Type of VCCs [1]? 0
ATM-I/F 0 QoS>
```

Remove

Utilice el mandato **remove** para eliminar la configuración de QoS de esta interfaz ATM.

Sintaxis:

remove

Ejemplo:

Configuración de la Calidad de los servicios (QoS)

```
ATM-I/F 0 QoS> remove
WARNING: This option deletes the QoS configuration.
        To re-configure use any of the SET options.
Should the ATM Interface QoS configuration be deleted? [No]: yes
Deleted QoS SRAM record successfully
ATM-I/F 0 QoS>
```

Acceso a los mandatos de supervisión de QoS

Utilice el mandato **feature** del proceso GWCON para acceder a los mandatos de supervisión de Calidad de los servicios. Entre **feature** seguido del número de característica (6) o del nombre corto (QoS). Por ejemplo:

```
+feature qos
Quality of Service (QoS) - User Monitoring
QoS+
```

Una vez que haya accedido al indicador de supervisión de QoS, puede seleccionar la supervisión de un LE Client específico. Para regresar al indicador GWCON en cualquier momento, entre el mandato exit en el indicador de supervisión de QoS.

Por otra parte, puede acceder a la Supervisión de QoS de un LE Client, de la manera siguiente:

1. En el indicador GWCON (+), entre el mandato de red y el número de interfaz de LE Client.
2. En el indicador de supervisión de LE Client, entre **qos-information**.

Ejemplo:

```
+network 3
ATM Emulated LAN Monitoring
LEC+qos information
LE Client QoS Monitoring
LEC 3 QoS+
```

Mandatos de supervisión de Calidad de los servicios

Esta sección resume los mandatos de supervisión de QoS. Entre estos mandatos en el indicador QoS+.

Tabla 40. Resumen de los mandatos de supervisión de la Calidad de los servicios (QoS)

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado "Cómo obtener ayuda" en la página xxxiv.
le-client	Le permite acceder al indicador LE Client QoS console + para el LE Client seleccionado.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página xxxiv.

Mandatos de supervisión de QoS de LE Client

Esta sección resume los mandatos de supervisión de QoS de LE Client. Entre los mandatos desde el indicador LEC num QoS+.

Tabla 41. Resumen de los mandatos de supervisión de QoS de LE Client

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxiv.
List	Lista la información actual de QoS de LE Client. Las opciones incluyen: parámetros de configuración, TLV, VCC y estadísticas.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiv.

List

Utilice el mandato **list** para listar la información relativa a QoS de este LE Client.

Sintaxis:

list configuration-parameters
 data-direct-VCCs (información detallada)
 statistics
 tlv-information
 vcc-information

configuration-parameters

Lista los parámetros de configuración de QoS. Dado que los parámetros pueden configurarse para un LE Client, la interfaz ATM o la ELAN, estos parámetros se visualizan con un conjunto resuelto de parámetros que el LE Client utiliza.

le-client Los parámetros configurados para este LE Client que se obtienen de los registros de la SRAM. Si los registros de la SRAM contienen un conjunto de parámetros no válido, esta columna no visualizará ningún valor de parámetro.

ATM Interface

Los parámetros configurados para la interfaz ATM utilizada por este LE Client. Estos parámetros se obtienen de los registros de la SRAM locales. Si los registros de la SRAM contienen un conjunto no válido de parámetros, esta columna no visualizará ningún valor de parámetro.

From LECS

Los parámetros recibidos por este LE Client desde el LE Configuration Server. Los parámetros se reciben como TLV individuales en el mensaje de control LE_CONFIGURE_RESPONSE.

Configuración de la Calidad de los servicios (QoS)

- used** El conjunto resuelto de parámetros de tráfico que se utilizarán para estas VCC Data Direct. Si no se configura ninguna de las entidades con los parámetros de QoS, los parámetros USED representan los parámetros por omisión. Si los parámetros se configuran para una entidad por lo menos, se resuelven de la manera siguiente:
- Si sólo el LE Client o la interfaz ATM se configura con parámetros, y `accept-parms-from-lecs` es FALSE o no se ha recibido ningún parámetro de LECS, se utilizan los parámetros del LE Client configurado o de la interfaz ATM.
 - Si tanto el LE Client como la interfaz ATM han configurado parámetros, se utilizan los parámetros de LE Client.
 - Si `accept-parms-from-lecs` es TRUE y se han recibido parámetros del LECS, los parámetros de LE Client (o el valor por omisión, si no se ha configurado el LE Client) se combinan con los recibidos del LECS para formar un conjunto completo de los seis primeros parámetros de QoS descritos en “Parámetros de configuración de QoS” en la página 286.
 - Si el conjunto de los seis primeros parámetros de QoS descritos en “Parámetros de configuración de QoS” en la página 286 contiene una combinación no válida, se rechazan los parámetros del LECS. Tenga en cuenta que los distintivos `negotiate-qos` y `validate-pcr-of-best-effort-vccs` se validan de forma independiente.

Ejemplo:

LEC 1 QoS+ list configuration parameters

ATM LEC Configured QoS Parameters				
QoS	LEC	ATM-IF	FROM	
PARAMETER	USED	SRAM	SRAM	LECS
Max Reserved Bandwidth (cells/sec) :	23584	23584	0	none
(Kbits/sec) :	10000	10000	0	none
VCC Type	ResvBW	ResvBW	BstEft	0
Peak Cell Rate	18867	18867	365566	365566
(Kbits/sec) :	8000	8000	155000	155000
Sustained Cell Rate ...	18867	18867	365566	none
(Kbits/sec) :	8000	8000	155000	none
QoS Class	4	4	0	none
Max Burst Size	95	95	0	none
(frames) :	1	1	0	none
Validate PCR of Best-Effort VCCs . :	no	no	n/a	none
Enable QoS Negotiation	yes	yes	n/a	none
Accept QoS Parameters from LECS .. :	yes	yes	n/a	n/a

(BstEft = Best Effort, ResvBW = Reserved Bandwidth)
(n/a = not applicable, none = no value is specified)

LEC 1 QoS+

data-direct-vccs (información detallada)

Esta opción lista la información de VCC Data Direct de este LE Client. También se lista información similar utilizando **list vcc-information**.

Ejemplo:

LEC 1 QoS+ list data direct vccs

```
LEC Data Direct VCCs - QoS Information
=====
```

```
Conn Handle = 80, VPI = 0, VCI = 546
Connection Type = RETRIED CONNECTION PARAMETERS
TrafficType     = BEST EFFORT VCC
PCR             = 58962 (25 Mbps)
SCR             = 58962 (25 Mbps)
QoS Class      = 0
Max Burst Size = 0
```

```
Conn Handle = 78, VPI = 0, VCI = 544
Connection Type = PARAMETERS SET BY DESTINATION
TrafficType     = RESERVED BANDWIDTH VCC
PCR             = 58962 (25 Mbps)
SCR             = 16509 (7 Mbps)
QoS Class      = 1
Max Burst Size = 95
```

LEC 1 QoS+

statistics Se mantienen unos contadores para las siguientes estadísticas:

Successful QoS Connections

Número de conexiones RESERVED-BANDWIDTH establecidas por el LE Client.

Successful Best-Effort Connections

Número de conexiones BEST-EFFORT establecidas por el LE Client.

Failed QoS Connections

Número de peticiones de conexión RESERVED-BANDWIDTH realizadas por el LE Client que han fallado.

Failed Best-Effort Connections

Número de peticiones de conexión BEST-EFFORT realizadas por el LE Client que han fallado.

QoS Negotiation Applied

Número de veces que se ha aplicado la extensión de negociación de QoS. Los parámetros se negocian si el LE Client recibe los parámetros de LE Client de destino en un mensaje de control LE_ARP_RESPONSE.

PCR Proposal (IBM) Applied

Número de veces que se ha aplicado la IBM Peak Cell Rate Proposal. Esta propuesta recomienda el uso de parámetros de velocidad específicos si se realiza la señalización a 100 Mbps, ó 155 Mbps para las conexiones BEST-EFFORT. Esto permite que otros productos IBM participantes (por ejemplo, los adaptadores ATM de 25 Mbps) rechacen una conexión basada en las velocidades mayores de célula señalizadas.

QoS Connections Accepted

Número de conexiones RESERVED-BANDWIDTH aceptadas por este LE Client.

Best-Effort Connections Accepted

Número de conexiones BEST-EFFORT aceptadas por este LE Client.

Configuración de la Calidad de los servicios (QoS)

QoS Connections Rejected

Número de peticiones de conexión RESERVED-BANDWIDTH recibidas por el LE Client que se han rechazado.

Best-Effort Connections Rejected

Número de peticiones de conexión BEST-EFFORT recibidas por el LE Client que se han rechazado.

Rejected due to PCR Validation

Número de conexiones BEST-EFFORT rechazadas por el LE Client, debido a la validación de la Velocidad mayor de célula, cuando el parámetro validate-pcr-of-best-effort-vccs es TRUE.

Ejemplo:

```
LEC 1 QoS+ 1i stat
```

```
QoS Statistics: of Data Direct Calls Placed by the LEC
```

```
-----  
Successful QoS Connections           = 0  
Successful Best-Effort Connections   = 1  
Failed QoS Connections               = 1  
Failed Best-Effort Connections       = 1  
Qos Negotiation Applied              = 0  
PCR Proposal (IBM) Applied           = 0
```

```
QoS Statistics: of Data Direct Calls Received by the LEC
```

```
-----  
QoS Connections Accepted             = 1  
Best-Effort Connections Accepted     = 0  
QoS Connections Rejected             = 0  
Best-Effort Connections Rejected     = 0  
Rejected due to PCR Validation        = 0
```

```
LEC 1 QoS+
```

tlv-information

Lista el IBM Traffic Information TLV que este LE Client ha registrado con el LE Server. El TLV sólo se registra si el LE Client está participando en la negociación de QoS.

Ejemplo:

```
LEC 1 QoS+ 1ist tlv
```

```
Traffic Info TLV of the LEC (registered with the LES)
```

```
-----  
TLV Type .....= 268458498  
TLV Length .....= 24  
TLV Value:  
Maximum Reserved Bandwidth = 23584 cells/sec (10 Mbps)  
Data Direct VCC Type..... = RESERVED BANDWIDTH VCC  
Data Direct VCC PCR..... = 18867 cells/sec (8 Mbps)  
Data Direct VCC SCR..... = 18867 cells/sec (8 Mbps)  
Data Direct VCC QoS Class = 4  
Maximum Burst Size         = 95 cells (1 frames)
```

```
LEC 1 QoS+
```

vcc-information

Lista todas las VCC activas del LE Client. La información incluye los parámetros de tráfico de las conexiones. Para las conexiones BEST-EFFORT, se visualiza la Velocidad sostenida de célula, que debe ser igual que la Velocidad mayor de célula, mientras que la Clase de QoS y el Tamaño máximo de ráfaga se visualizan con el valor 0.

Las entradas del Descriptor de parámetro son:

Configuración de la Calidad de los servicios (QoS)

SrcParms

Parámetros de una conexión establecida por este LE Client.

DestParms

Parámetros de una conexión recibida por este LE Client.

NegoParms

Parámetros de una conexión establecida por este LE Client para el que se ha utilizado la Negociación de QoS.

RetryParms

Parámetros de una conexión establecida por este LE Client, después de tener por lo menos una anomalía.

Ejemplo:

LEC 1 QoS+ 1i vcc

LEC VCC Table

=====

Conn Index	Conn Handle	VPI	VCI	Conn Type	Status	VCC Type	PCR (kbps)	SCR (kbps)	QoS Class	Burst Size (cells)	Parameters Descriptor
2)	69	0	535	Cntrl	Ready	BstEft	155000	155000	0	0	SrcParms
3)	71	0	537	Cntrl	Ready	BstEft	0	0	0	0	DestParms
4)	72	0	538	Mcast	Ready	BstEft	155000	155000	0	0	SrcParms
5)	74	0	540	Mcast	Ready	BstEft	0	0	0	0	DestParms
6)	78	0	544	Data	Ready	ResvBW	25000	7000	1	95	DestParms

LEC 1 QoS+

Configuración de la Calidad de los servicios (QoS)

Utilización de la característica de política

Este capítulo describe cómo interactúa la característica de política con otros componentes de software de direccionador para tomar decisiones acerca de QOS, la seguridad, o ambas cosas. También describe los conceptos y los mandatos de configuración específicos relativos a la característica de política. La característica de política también permite la utilización de un servidor de directorios LDAP como depósito central para la información sobre política. Los conceptos y los pasos de configuración que son necesarios para habilitar las funciones de LDAP también se describen en este capítulo. En los temas siguientes se analizan estos conceptos y la manera como los direccionadores aplican las políticas; asimismo se proporcionan algunos ejemplos.

- “Visión general de la política”
- “Interacción entre LDAP y la base de datos de políticas” en la página 315
- “Reglas de generación” en la página 319
- “Ejemplos de configuración” en la página 320

Visión general de la política

La característica de política facilita la gestión del tráfico de IPv4 en una red. Puede configurar políticas para reglas de filtros muy sencillas (eliminar o pasar), o para situaciones complejas de seguridad y QOS. La combinación de varias políticas determina cómo gestionarán los direccionadores el tráfico de IPv4 en una red.

Decisión y aplicación de una política

La implementación de políticas en esta familia de direccionadores constituye la base de las decisiones sobre políticas y los medios para aplicarlas. Se suele hacer referencia a estos conceptos como punto de decisión de política (PDP) y punto de aplicación de política (PEP).

La base de datos de políticas, que reside en la memoria del direccionador, se compone del conjunto de las políticas cargadas desde la configuración local y las políticas que se han leído desde LDAP. La base de datos de políticas se construye con las siguientes condiciones:

- Volver a cargar o a iniciar el dispositivo
- Mandato Talk 5 **reset database**
- Renovación automática
- Petición de definición de SNMP

La base de datos de políticas sirve como PDP y consiste en un conjunto de políticas que determinan cómo los componentes relacionados con la característica de política gestionan los paquetes. Cuando una política da como resultado una decisión (basada en información tal como la hora del día, la información sobre paquetes IP e información específica del protocolo como la identificación), la decisión se pasa al componente de aplicación (PEP) para que ejecute la acción. La Figura 26 en la página 308 muestra la relación entre estos componentes.

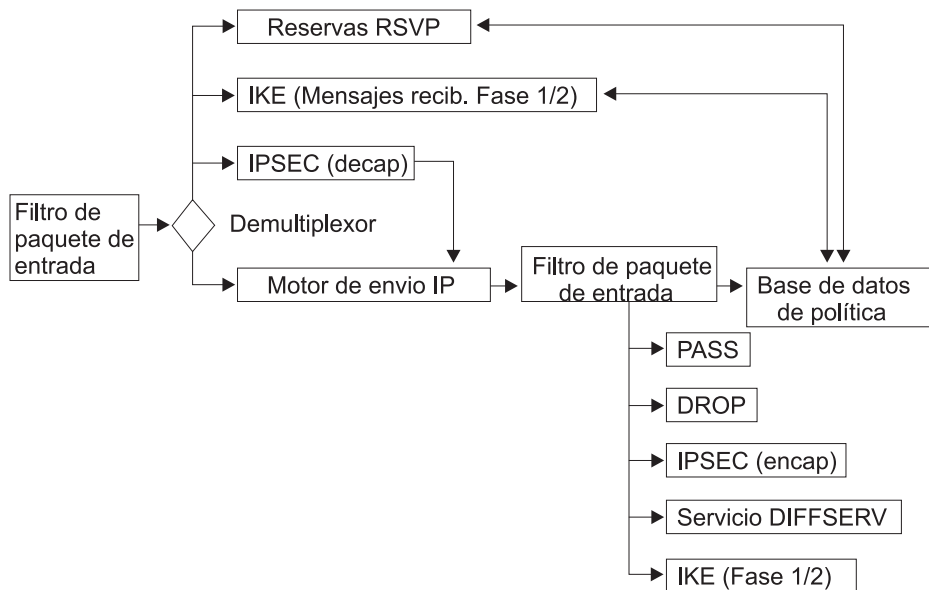


Figura 26. Flujo de paquetes IP y la base de datos de políticas

Decisión de política y flujo de paquetes

En primer lugar, los paquetes IP deben pasar el filtro de paquetes de entrada, antes de que pueda realizarse ninguna otra acción. Si el filtro de paquetes de entrada tiene reglas, se puede realizar alguna acción en el paquete. Si hay una coincidencia de filtro que excluye el paquete, o no se ha encontrado ninguna coincidencia en el filtro de paquetes de entrada, el paquete es eliminado.

Si el paquete pasa el filtro de paquetes de entrada, va a un filtro demultiplexor, que comprueba si el paquete tiene un destino local. Si lo tiene, según el tipo de paquete, lo pasa a otros módulos. Estos módulos pueden ser IPSec, IKE, RSVP u otros. Si el paquete tiene un destino local para IPSec, IKE o RSVP, estos módulos pueden consultar la base de datos de políticas para determinar la acción que se debe tomar.

Si el paquete no tiene un destino local, se entrega al motor de reenvío y se toma una decisión de direccionamiento. Si la decisión de direccionamiento no elimina el paquete (el Direccionamiento basado en la política puede decidir eliminar el paquete), éste irá al filtro de paquetes de salida. Si hay reglas de filtro en el paquete de salida, se puede realizar la conversión de direcciones (NAT) en el paquete, se puede pasar o se puede eliminar. Si no hay reglas de filtro, se pasa el paquete. Si hay reglas de filtro y no se encuentra ninguna coincidencia, se elimina el paquete. Si el paquete pasa el filtro de Paquetes de salida, el Motor IP consulta la base de datos de políticas para determinar si debe realizarse alguna otra acción en este paquete.

Nota: Si los filtros de paquetes de entrada y de salida están habilitados para una o varias interfaces, y se espera que los paquetes que la base de datos de política va a controlar atraviesen estas interfaces, debe haber una regla de filtros que incluya estos paquetes en los filtros de entrada y de salida, para que no se eliminen antes de que se consulte la base de datos de política. Se sugiere utilizar la base de datos de políticas para configurar todas las reglas de pasar y eliminar, y no utilizar los filtros de paquetes.

Consultas de política de IP

Cuando el motor de reenvío de IP consulta la base de datos de políticas, pueden devolverse los siguientes tipos de combinaciones de decisiones:

- No se ha encontrado ninguna coincidencia—pasar paquete
- Se ha encontrado una coincidencia—eliminar paquete
- Se ha encontrado una coincidencia—pasar paquete
- Se ha encontrado una coincidencia—asegurar el paquete en el túnel manual de IPsec x
- Se ha encontrado una coincidencia—asegurar el paquete en el túnel de IPsec negociado IKE x
- Se ha encontrado una coincidencia—iniciar negociaciones ISAKMP para fase 1 y 2, eliminar paquete
- Se ha encontrado una coincidencia—proporcionar QoS DiffServ x, asegurar paquete con IPsec

Consultas de política de IPsec

Si IPsec recibe un paquete, en primer lugar debe descapsularlo y después decidir si el paquete ha llegado al túnel de IPsec correcto (a menudo se llama a esto comprobación de conformidad). Se realiza consultando la base de datos de políticas. La base de datos de políticas puede devolver los tipos de decisiones siguientes para esta consulta:

- Comprobación de conformidad aprobada—reenviar el paquete
- Comprobación de conformidad fallida—eliminar el paquete

Decisiones de política de IKE

IKE puede consultar la base de datos de políticas y que se devuelvan las decisiones de política de IP de *fase 1* que aparecen en la Tabla 42.

Tabla 42. Consultas de fase 1 de IKE y decisiones devueltas

Tipo de consulta	Decisión
Mensaje 1 (Modalidad principal)	No se ha encontrado ninguna coincidencia, eliminar paquete
Mensaje 1 (Modalidad principal)	Se ha encontrado una coincidencia, negociar con política x de fase 1
Mensaje 5 (Modalidad principal)	No se ha encontrado ninguna coincidencia, detener negociaciones con similar, eliminar paquete
Mensaje 5 (Modalidad principal)	No se ha encontrado ninguna coincidencia, detener negociaciones con similar, eliminar paquete
Mensaje 5 (Modalidad principal)	Se ha encontrado una coincidencia, política 1 coincidente, finalizar fase 1
Mensaje 5 (Modalidad principal)	Se ha encontrado una coincidencia, política y coincidente, se detiene la fase 1 actual y se inicia una fase 1 nueva con política nueva
Mensaje 1 (Modalidad agresiva)	No se ha encontrado ninguna coincidencia, eliminar paquete
Mensaje 1 (Modalidad agresiva)	Se ha encontrado una coincidencia, política x coincidente

IKE puede consultar la base de datos de políticas y hacer que se devuelvan las decisiones de política de IP de fase 2 que aparecen en la Tabla 43 en la página 310.

Tabla 43. Consultas de fase 2 de IKE y decisiones devueltas

Tipo de consulta	Decisión
Mensaje 2 (respon-dedor)	No se ha encontrado ninguna coincidencia, eliminar paquete
Mensaje 2 (respon-dedor)	Se ha encontrado una coincidencia, negociar con política x

Decisiones de política de RSVP

Si un paquete es un mensaje de control de RSVP, RSVP consulta la base de datos de políticas para determinar si acepta la reserva o la rechaza. Si la acepta, RSVP determina qué atributos de la reserva limita, basándose en la política. Las políticas de la base de datos de políticas pueden controlar la duración de la reserva, la cantidad de ancho de banda que debe asignarse y el retardo mínimo garantizado.

Objetos de política

Una política se compone de un perfil, que contiene un conjunto de atributos de paquete sobre los que se basan las decisiones, las acciones que se realizan si los atributos de un paquete coinciden con los del perfil, y un período de validez durante el cual se toman las decisiones y se aplican las acciones. Estos elementos se explican con más detalles en los temas siguientes:

Las partes que componen una política son objetos con nombre diferenciados. Los objetos de política pueden hacerse referencia mutuamente, y componen una política como grupo de elementos relacionados. Al separar la información sobre configuración en objetos distintos y diferenciados, puede volver a utilizar muchos de ellos entre varias definiciones de política, ahorrando tiempo y reduciendo esfuerzos de mantenimiento. Los objetos de política individuales se analizan de manera detallada en los temas siguientes.

Política

El objeto de política describe qué condicionantes deben comprobarse y, si las comprobaciones son positivas, qué acciones deben aplicarse. La política realiza referencias con nombres al período de validez y al perfil. Para que la política sea válida, se necesitan estas referencias. La política debe realizar también una referencia con nombre a una o más de las acciones siguientes: un objeto de túnel de clave manual de IPsec o una acción de IPsec, ISAKMP, RSVP o DiffServ. Las combinaciones válidas son:

- Túnel de clave manual de IPsec
- Acción de IPsec para eliminar paquetes
- Acción de IPsec para pasar paquetes (sin seguridad)
- Acción de IPsec para asegurar paquetes, acción de ISAKMP
- Acción de DiffServ (eliminar)
- Túnel de clave manual de IPsec y acción de DiffServ (pasar)
- Acción de IPsec para asegurar paquetes, acción de ISAKMP o DiffServ (pasar)

- Acción de RSVP
- Acción de RSVP y de DiffServ (pasar)

Nota: En estas combinaciones, no puede haber un túnel manual de IPSec en la misma definición de política como acción de IPSec (túnel de IPSec negociado por IKE) y una acción de RSVP no se debe asociar a ninguna clase de acción de IPSec. Si una acción de IPSec para asegurar paquetes se asocia a una política, debe asociar también una acción de ISAKMP con la política.

Cada política tiene un número de prioridad asociado (cuanto mayor sea el número del atributo de prioridad, mayor será la prioridad). La prioridad determina si esta política tiene preferencia sobre otra. Lo normal es que sólo tenga que definirlo si existe algún tipo de conflicto entre los perfiles de dos o más políticas. La política que tenga el perfil más específico deberá tener también una prioridad mayor. Por ejemplo, suponga que una política específica que se debe asegurar el tráfico de la subred A a la subred B con IPSec (DES), mientras que otra política específica que el tráfico desde el punto a' (un sistema principal determinado en la subred A) a la subred B debe asegurarse con IPSec (3DES). La política más específica (a' a B) debe tener una prioridad mayor que la política con A a B.

Es una buena idea designar los valores de prioridad iniciales que tengan 5 o más dígitos, además de dejar espacio para especificar valores de prioridad adicionales para conflictos posteriores entre políticas. Cada política tiene también un atributo habilitado, que determina si debe habilitarse la política cuando se carga en la base de datos de políticas. Si se encuentra una coincidencia de política durante una búsqueda en la base de datos de políticas, pero la política está inhabilitada, se aplica la siguiente política más específica.

Perfil

El perfil determina qué información va a utilizarse para seleccionar una política determinada. El perfil consiste en la información de las direcciones de origen y de destino, la información de protocolo y la información de los puertos de origen y de destino.

Nota: Al definir políticas para IPSec/ISAKMP, cada pasarela que proporciona la seguridad debe tener una política para definir la asociación de seguridad. El perfil en cada pasarela debe asociar el origen con el destino, y el destino con el origen. El perfil para una política de IPSec debe especificar la dirección de origen como el tráfico que se va a encapsular en el túnel y la dirección de destino debe estar en el extremo remoto del túnel.

El perfil también puede seleccionarse según el byte de tipo de servicio (TOS) y la dirección IP de entrada y salida. Por omisión, un paquete recibido en cualquier interfaz de entrada y que sale en cualquier interfaz de salida, se compara con los otros selectores. En algunos casos, puede necesitar la flexibilidad para especificar exactamente las interfaces a las que debe llegar el paquete, así como la interfaz en la que el paquete debe salir. Si lo desea, debe añadir objetos de par de interfaces y asociar el nombre de grupo para los objetos de par de interfaces con el perfil. Asigne objetos de par de interfaces a un grupo dándoles el mismo nombre. Esto le permite especificar combinaciones tales como (cualquier paquete que llegue a IPaddrX y salga en cualquier interfaz *O* cualquier paquete que llegue a cualquier interfaz y salga en IPaddrX). Esto resulta especialmente útil si define una regla de eliminación general para una interfaz pública.

Par de interfaces: Identifica la interfaz de entrada y la de salida. Especifique las direcciones IP para la interfaz correspondiente a esta selección. El valor 255.255.255.255 implica cualquier interfaz.

Si desea utilizar el perfil para seleccionar una política de IPSec/ISAKMP, tiene la opción de especificar el ID local que debe enviarse durante la fase 1 y la lista de los ID remotos aceptables durante las negociaciones de la fase 1. Por omisión, el ID local es el punto final del túnel local para el tráfico de IPSec/IKE y la lista de ID remotos es *Any*. Opcionalmente, puede especificar el nombre de dominio calificado al completo (FQDN), el FQDN de usuario y el ID de clave. Normalmente, esto es suficiente porque se realiza la autenticación de las negociaciones de fase 1 de ISAKMP con certificados públicos o claves precompartidas. No obstante, en algunas situaciones de acceso remoto en las que se aplican comodines a la política para las direcciones de destino, puede ser preferible especificar una lista de los usuarios de acceso remoto a los que se debe permitir el acceso a los recursos de la red.

Todavía se realiza la autenticación de estos usuarios mediante los métodos de autenticación normales de ISAKMP, pero la base de datos de políticas realiza un paso de autenticación adicional, asegurando que el ID local enviado por el similar remoto coincide con uno de los ID especificados en el Grupo de usuarios remotos del perfil de la política. Esto es obligatorio si una autoridad de certificación (CA) pública administra certificados al público en general, y el administrador de red desea que sólo un conjunto específico de estos usuarios tenga acceso (por ejemplo, los empleados de la compañía). El grupo de usuarios remotos consiste en una lista de usuarios que pertenecen al mismo grupo. Estos usuarios se entran añadiendo uno o más *USER*. Un grupo de usuarios puede igualar el nombre de grupo para cada usuario. Entonces, y de manera opcional, este grupo se puede asociar a un perfil.

Período de validez

El período de validez especifica la existencia de la política: el año, los meses del año, los días de la semana y las horas del día en que tendrá validez. Esta flexibilidad permite que el administrador de red especifique cuándo es válida una política; por ejemplo, “siempre” o “sólo este año, durante los meses de enero, febrero y marzo, de lunes a viernes y de las 9 AM a las 5 PM”. Cuando se invalida una política de la base de datos de políticas, se aplicará la siguiente política más específica. Por consiguiente, podría definir una política que especifique de lunes a viernes, de las 9 AM a las 5 PM, para asegurar todo el tráfico desde la subred A a la B, y el resto del tiempo se debe eliminar todo el tráfico de la subred A a la B. En este caso, la primera política debe tener una prioridad más alta (se especifica al entrar el mandato `Talk 5 add policy`).

Acción de DiffServ

La acción de DiffServ describe la calidad de servicio que debe proporcionarse a los paquetes que coincidan con una política que especifica una acción de DiffServ. Puede configurar la acción de DiffServ para eliminar paquetes. También puede utilizar la acción de DiffServ para correlacionar los paquetes con calidades relativas de servicio. Puede configurar el ancho de banda asignado como un porcentaje del ancho de banda de salida o como un valor absoluto medido en Kbps. Debe especificar si es la cola de mejor esfuerzo/asegurada o la cola de calidad superior la que realice la asignación de ancho de banda. Para obtener más información acerca de estas colas y cómo definir las, consulte “Utilización de la característica de Servicios

diferenciados” en la página 425 y “Configuración y supervisión de la característica de Servicios diferenciados” en la página 431.

La acción de DiffServ también especifica cómo marcar el byte TOS antes de que se envíe en la interfaz de salida. Por omisión, el byte TOS no está marcado. Es útil para marcar los paquetes en un punto de la red, según la información contenida en la cabecera de paquete IP. Una vez determinada la clasificación, dado que el marcado del byte TOS ya se ha efectuado, el resto de los saltos de la red sólo tienen que consultar el nuevo byte TOS para determinar cuál es el QoS que se aplica al paquete. Consultar sólo el byte TOS es mucho más eficaz y puede ser necesario para conseguir un rendimiento elevado en la red principal de DiffServ.

Acción de RSVP

La acción de RSVP especifica si se permiten o se deniegan los flujos de RSVP, si se realiza una reserva de RSVP y la petición de reserva coincide con el perfil de la política. Si desea permitir la reserva, la acción de RSVP declara también la duración permitida de la reserva, el ancho de banda permitido y, de manera opcional, una referencia a una acción de DiffServ. La referencia a la acción de DiffServ permite que RSVP determine cómo marcar el byte TOS antes de que el paquete salga del direccionador. Esto es útil cuando los paquetes pasan de una red RSVP a una red DiffServ. RSVP puede proporcionar la QoS hasta el límite de RSVP y, entonces, marcar el byte TOS de la manera adecuada, de forma que la red DiffServ pueda aplicar el ancho de banda correcto.

Acción de IPSec

La acción de IPSec puede especificar una acción de eliminar, pasar o asegurar. Si la acción es eliminar, se eliminarán todos los paquetes que coincidan con esta política. Si la acción es pasar sin seguridad, todos los paquetes se pasarán al descubierto. Si la acción es pasar con seguridad, se asegurarán todos los paquetes mediante la asociación de seguridad (SA) especificada por esta acción. La acción de IPSec contiene también las direcciones IP de los puntos finales de túnel para las SA de túnel de IPSec e IKE.

Las propuestas de IPSec a las que hace referencia la acción de IPSec determinan los atributos de la SA. La acción de IPSec puede especificar varias propuestas de IPSec, que se envían y comprueban en el orden en que se han especificado. Tener varias propuestas en una acción de IPSec permite que la configuración contenga todas las combinaciones de seguridad aceptables, reduciendo así el número de discrepancias potenciales en la configuración entre varias pasarelas VPN.

Propuesta de IPSec

La propuesta de IPSec contiene la información que la transformación de ESP, AH (o ambas) proponen o comprueban durante las negociaciones de la fase 2 de ISAKMP. Si necesita un secreto perfecto de reenvío (un nuevo cálculo Diffie Hellman), la propuesta de IPSec identifica qué grupo DH se debe utilizar. Las transformaciones a las que hace referencia la propuesta de IPSec se envían o se comparan en el orden en que se han especificado. La primera transformación de ESP o AH de la lista debe ser aquella cuyo uso es el más adecuado. Si hay más de una transformación en la lista, cada una de ellas se compara con la lista de transformaciones del similar para encontrar una coincidencia. Si ninguna de las transformaciones configuradas coincide con la lista del similar, la negociación fallará. La propuesta de IPSec puede listar una combinación de transformaciones de AH y ESP, pero las únicas combinaciones válidas son:

Utilización de la característica de política

- Lista sólo de AH (modalidad de túnel o de transporte)
- Lista sólo de ESP (modalidad de túnel o de transporte)
- Lista de AH (modalidad de transporte) y lista de ESP (modalidad de túnel)

Transformación de IPSec

Los atributos de la transformación de IPSec contienen información acerca de los parámetros de cifrado y autenticación de IPSec; asimismo, también especifican con qué frecuencia se renuevan las claves. La transformación es AH (sólo autenticación) o ESP (cifrado, autenticación, o ambas), y puede configurarse para operar en la modalidad de túnel o de transporte.

Acción de ISAKMP

La acción de ISAKMP especifica la información de gestión de claves para la fase 1. Especifica si se deben iniciar las negociaciones de fase 1 en la modalidad principal (proporciona protección de identidad) o agresiva. También especifica si debe negociarse la asociación de seguridad de fase 1 al arrancar el dispositivo o según la demanda. La acción de ISAKMP también debe hacer referencia a una o más propuestas de ISAKMP. La primera referencia debe ser a la propuesta de ISAKMP que resulte más aceptable.

Propuesta de ISAKMP

La propuesta de ISAKMP especifica los atributos de cifrado y autenticación de la asociación de seguridad de la fase 1. También especifica cuál es el grupo Diffie Hellman que se debe utilizar para generar las claves y la existencia de la asociación de seguridad de la fase 1. Debe seleccionar el método de autenticación en la propuesta de ISAKMP. Puede ser la modalidad de clave precompartida o de certificado.

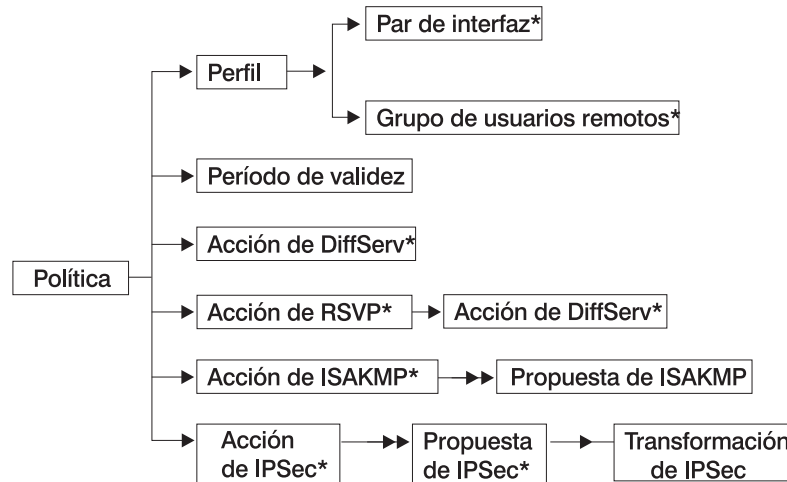
Usuario

Debe configurar un usuario (USER) para cualquier política que utilice una negociación de ISAKMP con la clave precompartida como método de autenticación. La configuración de USER identifica la clave precompartida que se va a utilizar para el similar ISAKMP. El objeto usuario contiene la información identificativa para un similar ISAKMP remoto, a saber: dirección IP, FQDN, FQDN de usuario o ID de clave, y qué método desea utilizar el usuario para realizar la autenticación. Puede seleccionar la modalidad de clave precompartida o de certificado. Si selecciona la clave precompartida, debe especificar también si la clave precompartida se debe entrar en formato ASCII o hexadecimal, así como el valor de la clave. Los USER se pueden agrupar asignándoles al mismo nombre de grupo. Entonces, y de manera opcional, este grupo se puede asociar a un perfil de política para realizar una consulta de política más rigurosa para la fase 1.

Túnel de clave manual de IPSec

El túnel de clave manual de IPSec es una configuración estática de los parámetros de cifrado y autenticación. No se realiza ninguna negociación para el túnel, de manera que ambos similares deben tener exactamente la misma configuración. Las claves se entran como parte de esta configuración y deben coincidir en ambos lados del túnel. Dado que no se realiza ninguna negociación en esta modalidad, las claves no se renuevan nada. Para obtener información acerca de los túneles de clave manual de IPSec, vea el análisis de la característica IPSec en la sección "Utilización de Seguridad de IP" en la página 367.

La Figura 27 en la página 315 muestra la relación entre los objetos de configuración de política.



Notas:

1. La → indica una referencia única.
2. La →→ indica una referencia múltiple.
3. La * indica una referencia opcional.
4. En una política de seguridad para ISAKMP/IPSec, el perfil de tráfico define el tráfico que fluye al túnel seguro.

Figura 27. Relación de objetos de configuración de política

Interacción entre LDAP y la base de datos de políticas

Esta familia de direccionadores permiten que un servidor LDAP (Lightweight Directory Access Protocol) sea el depósito de la información sobre política (la base de datos de políticas). LDAP es un protocolo que permite buscar en un servidor de directorios y modificarlo. LDAP es una versión ligera del estándar X.500. Los direccionadores dan soporte a la capacidad de buscar (pero no modificar) información en el servidor de directorios. El agente de búsqueda de política en el direccionador recupera toda la información existente en el servidor de directorios que está concebida para ese dispositivo. Cualquier servidor LDAP que opere con LDAP Versión 2 ó 3, trabaja con la implementación en el direccionador. Una ventaja importante de utilizar un servidor de directorios para almacenar información sobre política, frente a otros métodos más tradicionales de almacenar configuraciones localmente, es la capacidad de realizar un cambio en un lugar y que este cambio se aplique en todos los dispositivos de la red extendida. Esto incluye los dispositivos del dominio administrativo y los situados más allá de los límites públicos.

Por ejemplo, suponga que tiene una definición de transformación de IPsec que reside en el directorio. Si desea modificar la política empresarial de cifrado, de DES a 3DES, normalmente esto exigiría un cambio en todas las configuraciones de dispositivos a través de los límites de cada red. Si utiliza el directorio para desplegar las políticas, sólo tendrá que modificar una transformación de IPsec. Entonces, cada dispositivo habilitado por la política en la red, tendría que reconstruir la base de datos. En otro ejemplo distinto, suponga que tiene que modificar una acción de DiffServ denominada "GoldService" para aumentar el valor del

ancho de banda del 40% al 45%. El servidor LDAP y la infraestructura de la política permiten estos tipos de cambios de configuración para un ajuste proporcional mucho mejor, reduciendo las discrepancias entre las configuraciones.

Si es el administrador de la red, también puede aprovechar la ventaja de renovar automáticamente la base de datos cada día a una hora determinada. Seleccione esta opción entrando el mandato **set refresh** de la característica de política. Puede especificar si la renovación está habilitada o no y, si está habilitada, la hora a la que se debe renovar la base de datos. Esta opción es útil para realizar cambios automatizados. Por ejemplo, suponga que debe añadir una política nueva, de tal manera que el departamento de marketing de su país pueda hablar a través de Internet con el departamento de desarrollo que está en Japón, y que las pasarelas de seguridad son SG1 y SG2. Basta con que entre esta información en el directorio y, a medianoche, SG1 y SG2 recogerán automáticamente este cambio si tienen la renovación automática habilitada.

El motor de búsqueda de LDAP le permite especificar el nivel de seguridad que se va a utilizar mientras construye la base de datos de políticas. Defina estas opciones de seguridad con el mandato **set default** de la característica de política. Las opciones son:

- Pasar todo el tráfico durante la búsqueda (valor por omisión).
- Eliminar todo el tráfico *excepto* las peticiones de búsqueda de política de LDAP y sus resultados.
- Eliminar todo el tráfico *excepto* las peticiones de búsqueda de política de LDAP y los resultados protegidos por IPSec.

En ciertas situaciones, basta con cualquiera de las dos primeras opciones. No obstante, si el tráfico de LDAP atravesará la infraestructura pública, debe asegurar y autenticar la información seleccionando la tercera opción. En tal caso, debe seleccionar las opciones de autenticación y cifrado de las fases 1 y 2. También debe entrar las direcciones IP para los puntos finales del túnel (servidores LDAP primario y secundario). Este túnel IKE/IPSec de rutina de carga se negociará antes de que se envíe tráfico de LDAP. Esta característica le permite establecer la configuración que se muestra en la Figura 28 en la página 317.

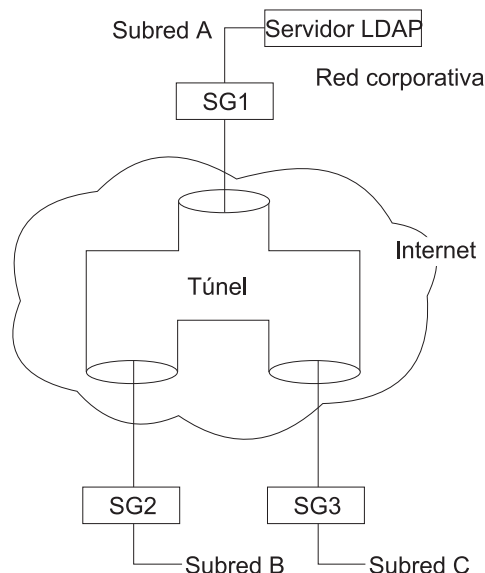


Figura 28. Seguridad del tráfico a través de Internet

Esta figura muestra un servidor LDAP en la Subred A de la red corporativa. SG1, SG2 y SG3 van a buscar sus políticas al servidor LDAP. La búsqueda de la política para SG2 y SG3 se produce a través de Internet y está protegida mediante IPsec.

La información de configuración necesaria para que la base de datos de política recupere las políticas del directorio es:

- Dirección IP de servidor primario (también se puede configurar un servidor secundario de reserva)
- Número de puerto en el que escucha el servidor (Nota: SSL y TLS no están soportados)
- Información del nombre de usuario y la contraseña, si es necesario
- Nombre distinguido básico del objeto DeviceProfile para este direccionador o clase de direccionadores.
- Información de política por omisión

Después de haber entrado esta información de configuración, la siguiente vez que se renueve la base de datos de políticas, se realizará un intento de interrogar la información sobre política al servidor de directorios. La base de datos de políticas permite una combinación de políticas configuradas localmente y reglas leídas del servidor LDAP. Si se descubre que dos reglas están en conflicto y tienen la misma prioridad, la regla leída de la configuración local tiene preferencia sobre la leída en el servidor de directorios.

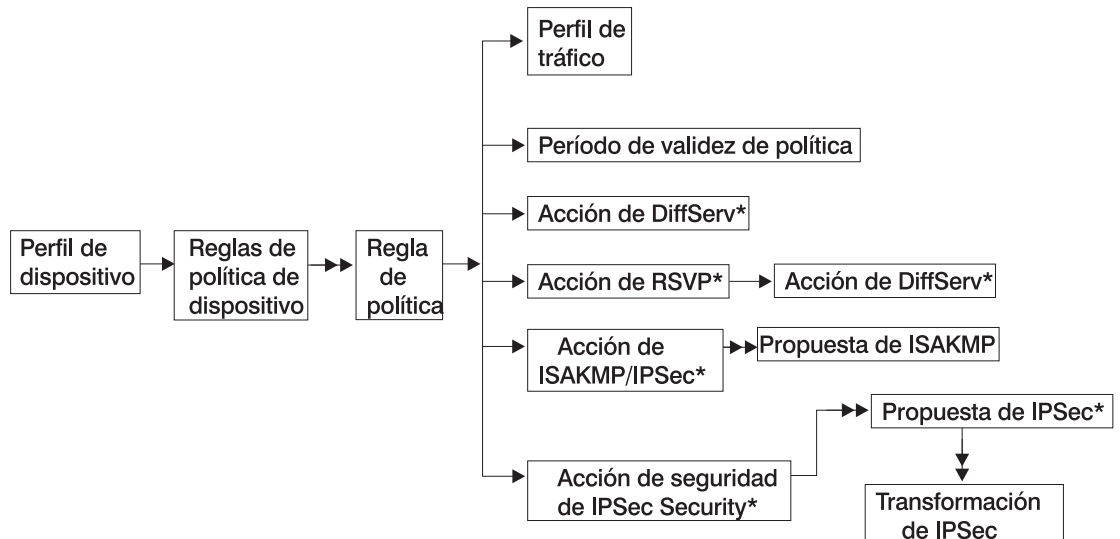
Esquema de política

El esquema LDAP es el conjunto de reglas e información que compone las definiciones de clases y atributos que determinan el contenido de las entradas del directorio. Normalmente, el esquema LDAP se escribe en la sintaxis de ASN1, similar a las MIB SNMP. El esquema de política al que esta familia de direccionadores da soporte, es un trabajo de los esfuerzos previos a los estándares realizados en IETF. Se basa en el trabajo de seguimiento estándar realizado por los Grupos de trabajo de IPsec y política en el IETF y el Grupo de trabajo de política en el DMTF. El esquema de política compara rigurosamente los objetos de

Utilización de la característica de política

configuración existentes en la característica de política en el direccionador. Los archivos de definición de definición de esquema de política y los archivos de configuración del servidor LDAP pueden encontrarse accediendo al siguiente URL:

<http://www.networking.ibm.com/support>. Seleccione el producto de direccionador que desea y seleccione el enlace *Downloads*. La Figura 29 muestra la estructura general del esquema de política.



Notas:

1. La \rightarrow indica una referencia única.
2. La $\rightarrow\rightarrow$ indica una referencia múltiple.
3. La * indica una referencia opcional.
4. En una política de seguridad para ISAKMP/IPSec, el perfil de tráfico define el tráfico que fluye al túnel seguro.

Figura 29. Estructura de esquema de política

DeviceProfile y DevicePolicyRules son dos objetos de clave en el esquema de política. Habilitan el agente de búsqueda de política para localizar las políticas necesarias para el dispositivo. DeviceProfile contiene información acerca de la dirección IP administrativa del dispositivo y una referencia obligatoria de DevicePolicyRules. Puede agrupar dispositivos en un DeviceProfile o cada dispositivo de la red puede tener su propio DeviceProfile. La elección que realice dependerá de si hay más de un dispositivo en la red que debe ir a buscar el mismo conjunto de reglas. Normalmente, esto no sucede en el caso de las pasarelas de seguridad, porque cada pasarela tiene un punto final de túnel diferente. Para los dispositivos que sean sólo QOS, es concebible que todos los dispositivos de un grupo lean el mismo conjunto de políticas.

El objeto DevicePolicyRules se recupera basado en el valor de DeviceProfile que se busca para el dispositivo. Una vez recuperado el objeto DevicePolicyRules, puede recuperarse la lista de PolicyRules para ese dispositivo. Si no se encuentra ningún objeto, o si se ha detectado un error durante una comprobación de coherencia en un objeto; después, la búsqueda se cancela anormalmente y se visualizan mensajes en ELS (mensajes PLCY) que identifican el error. Si se produce un error, el administrador de red puede configurar una de las siguientes elecciones para gestionarla:

- Suprima todas las políticas leídas localmente y regrese a una regla de eliminar o pasar todo
- Mantenga todas las políticas leídas localmente. Especifique esta opción con el mandato **set default** de la característica de política.

En cualquier caso, la búsqueda se intentará de nuevo en el intervalo de reintentos configurado. Si no se puede establecer contacto con el servidor LDAP primario, se intentará el servidor secundario al cabo de 5 intentos. Si no se puede establecer contacto con el servidor secundario, se intentará de nuevo el servidor primario al cabo de 5 intentos. Puede especificar el intervalo de reintentos con el mandato **set ldap retry-interval** de la característica de política. Si una búsqueda falla a causa de la latencia de red, puede cambiar el tiempo de espera de búsqueda, modificando el valor por omisión de 3 segundos, mediante el mandato **set ldap search-timeout** de la característica de política.

Reglas de generación

Configure una política para especificar cómo desea que opere la red. El direccionador convierte la información de política a un conjunto de reglas que se compara con los flujos de tráfico. En el pasado, puede haber hecho esto manualmente al definir filtros de paquetes de entrada y de salida para cada patrón de tráfico. La base de datos de política lo elimina, porque con ello sólo configuraría una única política.

La mayoría del trabajo se realiza internamente cada vez que se construye la base de datos de política. En algunos casos, un direccionador convierte una política directamente en una única regla. En el caso de ISAKMP/IPSec, convierte una política en cinco reglas. Se necesitan cinco reglas para cubrir las direcciones del tráfico (de entrada y salida) y para los flujos de control que se producen durante las negociaciones de las fases 1 y 2 de IKE. La relación entre las políticas y las reglas es la siguiente:

Una política DiffServ → Una regla DiffServ

Una política RSVP → Una regla RSVP

Una política ISAKMP/IPSec → Cinco reglas ISAKMP/IPSec

Ejemplo: Asegurar el tráfico de la subred A a la B; los puntos finales del túnel son SGa y SGb

1. Fase 1 de entrada (Perfil = SGb a SGa, Proto UDP, Puerto fuente 500, Puerto destino 500): esta regla es necesaria para filtrar las negociaciones de fase 1 de entrada desde el similar ISAKMP remoto, si el dispositivo funciona como un respondedor ISAKMP.
2. Fase 1 de salida (Perfil = SGa a SGb, Proto UDP, Puerto fuente 500, Puerto destino 500): esta regla es necesaria para filtrar la información de fase 1 que es necesaria si el tráfico inicia las negociaciones ISAKMP de fase 1. En este caso, el dispositivo funciona como iniciador de ISAKMP.

Utilización de la característica de política

3. Fase 2 de entrada (Perfil = SGb a SGa, Proto UDP, Puerto fuente 500, Puerto destino 500): esta regla es necesaria para filtrar el tráfico de fase 2 de entrada desde el similar ISAKMP remoto. Este tráfico es el resultado de que el similar remoto inicie una renovación o negociación inicial de fase 2. No es necesaria una regla de salida de fase 2, dado que el tráfico de salida (regla 5) empieza siempre las negociaciones, si son necesarias.
4. Tráfico al túnel seguro (Perfil = Subred A a Subred B): esta regla es necesaria para poner el tráfico no protegido en un túnel seguro. Si no se ha negociado la asociación de seguridad, también se reúne la regla de la fase 1 e IKE inicia las fases 1 y 2. Una vez que se hayan establecido las SA, los paquetes que coincidan con esta regla se entregarán a IPSec para su encapsulación y transmisión.
5. Tráfico desde el túnel seguro (Perfil = Subred B a Subred A): esta regla es necesaria para asegurar que los paquetes que deberían haber llegado en un túnel seguro, efectivamente han llegado en un túnel seguro. Si IPSec no ha descapsulado el paquete y encuentra esta regla, se elimina el paquete. Esta regla gestiona el tráfico enviado a la red.

Un túnel de clave manual IPSec → Dos reglas de IPSec

Ejemplo: Asegurar el tráfico de la subred A a la B; los puntos finales del túnel son SGa y SGb.

1. Tráfico al túnel seguro (Perfil = Subred A a Subred B): esta regla es necesaria para poner el tráfico no protegido en un túnel seguro. Éste es un túnel configurado estáticamente, por lo que siempre está disponible, y los paquetes que coincidan con esta regla se enviarán directamente a IPSec para su encapsulación y transmisión.
2. Tráfico desde el túnel seguro (Perfil = Subred B a Subred A): esta regla es necesaria para asegurar que los paquetes que deberían haber llegado en un túnel seguro, efectivamente han llegado en un túnel seguro. Si IPSec no ha descapsulado el paquete y encuentra esta regla, se elimina el paquete. Esta regla gestiona el tráfico enviado a la red.

Puede ver estas reglas utilizando el mandato `Talk 5 list rule`.

Ejemplos de configuración

Los siguientes ejemplos muestran cómo puede utilizar la característica de política para configurar los direccionadores en una red. En primer lugar, acceda a la característica de política, como se muestra a continuación:

```
* talk 6
Config>feature policy
IP Network Policy configuration
```

Política de IPSec/ISAKMP con QOS

Puede entrar información sobre política de dos maneras. La primera es definir los objetos de política individuales y agruparlos. Para utilizar este método, defina primero las transformaciones de IPSec y después la propuesta de IPSec (que hace referencia a las transformaciones de IPSec). A continuación, defina la acción de IPSec (que hace referencia a las propuestas de IPSec), y así sucesivamente hasta que haya definido la política por completo. Utilizando la Figura 30 como referencia, este método empezará por el lado derecho de los objetos de política y avanzará hacia la izquierda.

El segundo enfoque, que tal vez le parezca más sencillo, consiste en definir primero las opciones de política de alto nivel y, cuando se le solicite, entrar las definiciones para los objetos de política individuales mientras vaya trabajando. Después de la Figura 30 se muestra un procedimiento de configuración de ejemplo, y utiliza unos valores que corresponden a los de la figura. Utiliza el método de izquierda a derecha y empieza con el mandato **add policy**.

Si se ha definido anteriormente un objeto que satisface sus necesidades, puede volver a utilizarlo en vez de crear una definición nueva. Por ejemplo, si se ha configurado un período de validez de allTheTime para una política anterior, puede volver a utilizarlo. El siguiente procedimiento muestra el proceso entero, pero no muestra cómo se vuelve a utilizar información de política definida anteriormente. Para obtener un ejemplo de la utilización definida anteriormente, consulte “Política única de IPSec/ISAKMP” en la página 331.



Figura 30. Configuración de IPSec/ISAKMP con QOS

La situación de configuración de la política descrita en el texto siguiente corresponde a la perspectiva de un SG1. La instrucción de la política es la siguiente:

Asegurar el tráfico desde la subred 11 a la subred 12, siendo SG1 y SG2 los puntos finales del túnel, y proporcionar un QOS para el tráfico en este túnel mediante DiffServ GoldService

1. Añada la política.

```

Policy config>add policy
Enter a Name (1-29 characters) for this Policy []? examplePolicySecure11to12
Enter the priority of this policy (This number is used to
determine the policy to enforce in the event of policy conflicts) [5]? 10
  
```

2. No hay ningún perfil configurado, por lo que debe definir uno nuevo.

```

List of Profiles:
0: New Profile

Enter number of the profile for this policy [0]?
  
```

3. Nueva definición de perfil; en este caso, el tráfico que nos interesa va desde la subred 11 a la subred 12.

Utilización de la característica de política

```
Enter a Name (1-29 characters) for this Profile []? trafficFrom11NetTo12Net
Source Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]?
Enter IPV4 Source Address [0.0.0.0]? 11.0.0.0
Enter IPV4 Source Mask [255.0.0.0]?
Destination Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]?
Enter IPV4 Destination Address [0.0.0.0]? 12.0.0.0
Enter IPV4 Destination Mask [255.0.0.0]?
```

```
Protocol IDs:
 1) TCP
 2) UDP
 3) All Protocols
 4) Specify Range
```

```
Select the protocol to filter on (1-4) [3]?
Enter the Starting value for the Source Port [0]?
Enter the Ending value for the Source Port [65535]?
Enter the Starting value for the Destination Port [0]?
Enter the Ending value for the Destination Port [65535]?
Enter the Mask to be applied to the Received DS-byte [0]?
Enter the value to match against after the Mask has
been applied to the Received DS-byte [0]?
Configure local and remote ID's for ISAKMP? [No]:
Limit this profile to specific interface(s)? [No]:
```

Here is the Profile you specified...

```
Profile Name      = trafficFrom11NetTo12Net
sAddr:Mask=      11.0.0.0 : 255.0.0.0      sPort=   0 : 65535
dAddr:Mask=      12.0.0.0 : 255.0.0.0      dPort=   0 : 65535
proto            =                0 : 255
TOS              =                x00 : x00
Remote Grp=All Users
Is this correct? [Yes]:
```

4. Ha terminado con la definición de perfil y ha regresado al menú de configuración de política.

```
List of Profiles:
 0: New Profile
 1: trafficFrom11NetTo12Net
```

```
Enter number of the profile for this policy [1]? 1
```

5. No hay ningún período de validez configurado, por lo que debe definir uno nuevo.

```
List of Validity Periods:
 0: New Validity Period
```

```
Enter number of the validity period for this policy [0]?
```

6. Preguntas de la configuración del período de validez; en este ejemplo, el período de validez comprende desde las 9 AM a las 5 PM, de lunes a viernes durante todos los meses de 1999.

Enter a Name (1-29 characters) for this Policy Valid Profile []?

MonToFri-9am:5pm-1999

Enter the lifetime of this policy. Please input the information in the following format:

yyymmddhhmmss:yyymmddhhmmss OR '*' denotes forever.

[*]? **19990101000000:19991231000000**

During which months should policies containing this profile be valid. Please input any sequence of months by typing in the first three letters of each month with a space in between each entry, or type ALL to signify year round.

[ALL]?

During which days should policies containing this profile be valid. Please input any sequence of days by typing in the first three letters of each day with a space in between each entry, or type ALL to signify all week

[ALL]? **mon tue wed thu fri**

Enter the starting time (hh:mm:ss or * denotes all day)

[*]? **00:00:00**

Enter the ending time (hh:mm:ss)

[00:00:00]? **17:00:00**

Here is the Policy Validity Profile you specified...

```
Validity Name   = MonToFri-9am:5pm-1999
Duration       = 19990101000000 : 19991231000000
Months         = ALL
Days           = MON TUE WED THU FRI
Hours          = 09:00:00 : 17:00:00
```

Is this correct? [Yes]:

7. Ha terminado con la definición del período de validez y ha regresado al menú de configuración de política.

List of Validity Periods:

0: New Validity Period
1: MonToFri-9am:5pm-1999

Enter number of the validity period for this policy [1]? **1**

Should this policy enforce an IPSEC action? [No]: **yes**

8. Debe definir siempre una nueva acción de IPSec, ya que el punto final del túnel será siempre diferente. Las excepciones se producen si hay varios túneles entre dos mismas pasarelas y, en las configuraciones de acceso remoto con comodines, se desconoce la ubicación del punto final del túnel.

IPSEC Actions:

0: New IPSEC Action

Enter the Number of the IPSEC Action [0]?

9. Menú de acciones de IPSec.

Utilización de la característica de política

```
Enter a Name (1-29 characters) for this IPsec Action []? secure11NetTo12Net
List of IPsec Security Action types:
  1) Block (block connection)
  2) Permit

Select the Security Action type (1-2) [2]? 2
Should the traffic flow into a secure tunnel or in the clear:
  1) Clear
  2) Secure Tunnel
[2]?
Enter Tunnel Start Point IPV4 Address
[11.0.0.5]? 1.1.1.1
Enter Tunnel End Point IPV4 Address (0.0.0.0 for Remote Access)
[0.0.0.0]? 1.1.1.2
Does this IPSEC tunnel flow within another IPSEC tunnel? [No]:
Percentage of SA lifesize/lifetime to use as the acceptable minimum [75]?

Security Association Refresh Threshold, in percent (1-100) [85]?
Options for DF Bit in outer header (tunnel mode):
  1) Copy
  2) Set
  3) Clear
Enter choice (1-3) [1]?
Enable Replay prevention (1=enable, 2=disable) [2]?
Do you want to negotiate the security association at
system initialization(Y-N)? [No]:
You must choose the proposals to be sent/checked against during phase 2
negotiations. Proposals should be entered in order of priority.
```

10. No hay ninguna propuesta de IPsec definida, por lo que debe definir una nueva. Tenga en cuenta que, una vez definida la propuesta de IPsec, podrá volver a utilizarse entre varias acciones de IPsec.

```
List of IPSEC Proposals:
  0: New Proposal

Enter the Number of the IPSEC Proposal [0]?
```

11. Configuración de la propuesta de IPsec.

```
Enter a Name (1-29 characters) for this IPsec Proposal []? genP2Proposal
Does this proposal require Perfect Forward Secrecy?(Y-N)? [No]:
Do you wish to enter any AH transforms for this proposal? [No]:
Do you wish to enter any ESP transforms for this proposal? [No]: yes
```

12. No hay ninguna transformación de ESP configurada, por lo que debe definir una nueva. Una vez que haya definido la transformación de ESP, cualquier propuesta de IPsec puede volver a utilizarse.

```
List of ESP Transforms:
  0: New Transform

Enter the Number of the ESP transform [0]? 0
```

13. Configuración de la transformación de IPsec.

Enter a Name (1-29 characters) for this IPsec Transform []? **esp3DESswSHA**

List of Protocol IDs:

- 1) IPSEC AH
- 2) IPSEC ESP

Select the Protocol ID (1-2) [1]? **2**

List of Encapsulation Modes:

- 1) Tunnel
- 2) Transport

Select the Encapsulation Mode(1-2) [1]? **1**

List of IPsec Authentication Algorithms:

- 0) None
- 1) HMAC-MD5
- 2) HMAC_SHA

Select the ESP Authentication Algorithm (0-2) [2]? **2**

List of ESP Cipher Algorithms:

- 1) ESP DES
- 2) ESP 3DES
- 3) ESP CDMF
- 4) ESP NULL

Select the ESP Cipher Algorithm (1-4) [1]? **2**

Security Association Lifesize, in kilobytes (1024-65535) [50000]?

Security Association Lifetime, in seconds (120-65535) [3600]?

Here is the IPsec transform you specified...

```
Transform Name = esp3DESswSHA
Type =ESP      Mode =Tunnel      LifeSize= 50000 LifeTime= 3600
Auth =SHA      Encr =3DES
Is this correct? [Yes]:
```

14. Regrese al menú de propuestas de IPsec.

List of ESP Transforms:

- 0: New Transform
- 1: esp3DESswSHA

Enter the Number of the ESP transform [1]?

Do you wish to add another ESP transform to this proposal? [Yes]: **no**

Here is the IPsec proposal you specified...

```
Name = genP2Proposal
Pfs = N
ESP Transforms:
    esp3DESswSHA
Is this correct? [Yes]:
```

15. Regrese al menú de acciones de IPsec.

Utilización de la característica de política

List of IPSEC Proposals:

0: New Proposal
1: genP2Proposal

Enter the Number of the IPSEC Proposal [1]?

Are there any more Proposal definitions for this IPSEC Action? [No]:

Here is the IPSec Action you specified...

```
IPSECAction Name = secure11NetTo12Net
  Tunnel Start:End      =      1.1.1.1 : 1.1.1.2
  Tunnel In Tunnel      =      No
  Min Percent of SA Life =      75
  Refresh Threshold     =      85 %
  Autostart             =      No
  DF Bit                =      COPY
  Replay Prevention     =      Disabled
  IPSEC Proposals:
    genP2Proposal
```

Is this correct? [Yes]:

16. Regrese al menú de política.

IPSEC Actions:

0: New IPSEC Action
1: secure11NetTo12Net

Enter the Number of the IPSEC Action [1]? 1

17. Ha especificado un tipo de acción de IPSec seguro, por lo que debe identificar una acción ISAKMP para las negociaciones de fase 1. No hay ninguna definida, por lo que debe entrar una nueva. En la mayoría de los casos, una acción y propuesta de ISAKMP es suficiente para todas las políticas de seguridad.

ISAKMP Actions:

0: New ISAKMP Action

Enter the Number of the ISAKMP Action [0]?

18. Configuración de acción de ISAKMP.

Enter a Name (1-29 characters) for this ISAKMP Action []? genPhase1Action

List of ISAKMP Exchange Modes:

1) Main
2) Aggressive

Enter Exchange Mode (1-2) [1]?

Percentage of SA lifiesize/lifetime to use as the acceptable minimum [75]?

ISAKMP Connection Lifesize, in kilobytes (100-65535) [5000]?

ISAKMP Connection Lifetime, in seconds (120-65535) [30000]?

Do you want to negotiate the security association at

system initialization(Y-N)? [Yes]: **no**

You must choose the proposals to be sent/checked against during phase 1 negotiations. Proposals should be entered in order of priority.

19. No hay ninguna propuesta de ISAKMP configurada, por lo que debe crear una nueva.

List of ISAKMP Proposals:
 0: New Proposal

20. Configuración de la propuesta de ISAKMP.

Enter the Number of the ISAKMP Proposal [0]?
 Enter a Name (1-29 characters) for this ISAKMP Proposal []? **genP1Proposa1**

List of Authentication Methods:
 1) Pre-Shared Key
 2) RSA SIG

Select the authentication method (1-2) [1]? **2**

List of Hashing Algorithms:
 1) MD5
 2) SHA

Select the hashing algorithm(1-2) [1]? **2**

List of Cipher Algorithms:
 1) DES
 2) 3DES

Select the Cipher Algorithm (1-2) [1]? **2**
 Security Association Lifesize, in kilobytes (100-65535) [1000]?
 Security Association Lifetime, in seconds (120-65535) [15000]?

List of Diffie Hellman Groups:
 1) Diffie Hellman Group 1
 2) Diffie Hellman Group 2

Select the Diffie Hellman Group ID from this proposal (1-2) [1]?

Here is the ISAKMP Proposal you specified...

```
Name = genP1Proposa1
AuthMethod = Pre-Shared Key
LifeSize = 1000
LifeTime = 15000
DHGroupID = 1
Hash Algo = SHA
Encr Algo = 3DES CB
Is this correct? [Yes]:
```

21. Regrese a la configuración de acción de ISAKMP.

List of ISAKMP Proposals:
 0: New Proposal
 1: genP1Proposa1

Enter the Number of the ISAKMP Proposal [1]?
 Are there any more Proposal definitions for this ISAKMP Action? [No]:

Here is the ISAKMP Action you specified...

```
ISAKMP Name = genPhase1Action
Mode = Main
Min Percent of SA Life = 75
Conn LifeSize:LifeTime = 5000 : 30000
Autostart = No
ISAKMP Proposals:
    genP1Proposa1
Is this correct? [Yes]:
```

22. Regrese a la configuración de política.

You must enable and configure DiffServ in feature DS before QoS can be ensured for this policy

27. El paso final de este proceso consiste en añadir una definición de perfil USER para el similar ISAKMP remoto. Este paso no es necesario si las negociaciones de ISAKMP van a realizar la autenticación del similar con certificados públicos. No obstante, en el ejemplo anterior hemos elegido la clave precompartida como método de autenticación, por lo que debemos identificar al usuario y entrar la clave precompartida que esperamos que utilice el similar.

```
Policy config>add user
Choose from the following ways to identify a user:
  1: IP Address
  2: Fully Qualified Domain Name
  3: User Fully Qualified Domain Name
  4: Key ID (Any string)
Enter your choice(1-4) [1]?
Enter the IP Address that distinguishes this user
[0.0.0.0]? 1.1.1.2
Group to include this user in []? peers
Authenticate user with 1:pre-shared key or 2: Public Certificate [1]?
Mode to enter key (1=ASCII, 2=HEX) [1]?
Enter the Pre-Shared Key (an even number of 2-128 ascii chars):
Enter the Pre-Shared Key again (10 characters) in ascii:

Here is the User Information you specified...

Name      = 1.1.1.2
Type      = IPV4 Addr
Group     =peers
Auth Mode =Pre-Shared Key
Key(Ascii)=exampleKey
Is this correct? [Yes]:
```

28. Ahora se han completado los pasos de configuración de política. Si desea configurar DiffServ, IPSec o cualquier red o configuración de IP, debe realizarlo antes de que el túnel de IPSec esté en funcionamiento. El siguiente ejemplo del mandato list muestra la configuración que se acaba de completar. Para activar estas modificaciones, vuelva a cargar el dispositivo o entre el mandato Talk 5 **reset database** de la característica de política.

Utilización de la característica de política

```
Policy config>list all

Configured Policies....

Policy Name      = examplePolicySecure11to12
State:Priority   =Enabled      : 10
Profile         =trafficFrom11NetTo12Net
Valid Period    =MonToFri-9am:5pm-1999
IPSEC Action    =secure11NetTo12Net
ISAKMP Action   =genPhase1Action
DiffServ Action =GoldService
--More--

Configured Profiles....

Profile Name     = trafficFrom11NetTo12Net
sAddr:Mask=     11.0.0.0 : 255.0.0.0      sPort=   0 : 65535
dAddr:Mask=     12.0.0.0 : 255.0.0.0      dPort=   0 : 65535
proto          =                               0 : 255
TOS            =                               x00 : x00
Remote Grp=All Users
--More--

Configured Validity Periods

Validity Name    = MonToFri-9am:5pm-1999
Duration        = 19990101000000 : 19991231000000
Months         = ALL
Days           = MON TUE WED THU FRI
Hours         = 09:00:00 : 17:00:00
--More--

Configured DiffServ Actions....

DiffServ Name   = GoldService                Type =Permit

TOS mask:modify=x00:x00
Queue:BwShare  =Assured      : 40 %
--More--

Configured IPSEC Actions....

IPSECAction Name = secure11NetTo12Net
Tunnel Start:End =          1.1.1.1 : 1.1.1.2
Tunnel In Tunnel =          No
Min Percent of SA Life =          75
Refresh Threshold =          85 %
Autostart        =          No
DF Bit           =          COPY
Replay Prevention =          Disabled
IPSEC Proposals:
    genP2Proposal
--More--

Configured IPSEC Proposals....

Name = genP2Proposal
Pfs  = N
ESP Transforms:
    esp3DESswSHA
--More--

Configured IPSEC Transforms....

Transform Name = esp3DESswSHA
Type =ESP     Mode =Tunnel     LifeSize= 50000 LifeTime= 3600
Auth =SHA     Encr =3DES
--More--
```

Configured ISAKMP Actions....

```
ISAKMP Name      = genPhase1Action
  Mode           =                               Main
  Min Percent of SA Life =                       75
  Conn LifeSize:LifeTime =                     5000 : 30000
  Autostart      =                               No
  ISAKMP Proposals:
    genP1Proposal
```

--More--

Configured ISAKMP Proposals....

```
Name = genP1Proposal
  AuthMethod = Pre-Shared Key
  LifeSize   = 1000
  LifeTime   = 15000
  DHGroupID  = 1
  Hash Algo  = SHA
  Encr Algo  = 3DES CB
```

--More--

Configured Policy Users....

```
Name      = 1.1.1.2
Type      = IPV4 Addr
  Group    =peers
  Auth Mode =Pre-Shared Key
  Key(Ascii)=exampleKey
```

--More--

Configured Manual IPSEC Tunnels....

IPv4 Tunnels

ID	Name	Local IPv4 Addr	Rem IPv4 Addr	Mode	State
----	------	-----------------	---------------	------	-------

Política única de IPSec/ISAKMP

Un ejemplo de procedimiento de configuración, que viene a continuación de la Figura 31 y que utiliza valores que se corresponden con los de la figura, usa el método de izquierda a derecha y muestra cómo construir sobre el procedimiento de ejemplo anterior volviendo a utilizar la información que éste creó.



Figura 31. Configuración de IPSec y nueva utilización de una definición anterior

La situación de configuración de la política descrita en el texto siguiente corresponde a la perspectiva de SG1. La instrucción de la política en esta situación es:

Asegurar el tráfico desde la subred 11 a la subred 13 (únicamente tráfico TCP), siendo SG1 y SG3 los extremos del túnel, y no proporcionar ningún QOS.

Utilización de la característica de política

1. Añada la política.

```
Policy config>add policy
Enter a Name (1-29 characters) for this Policy []? examplePolicySecure11to13
Enter the priority of this policy (This number is used to
determine the policy to enforce in the event of policy conflicts) [5]? 10
List of Profiles:
  0: New Profile
  1: trafficFrom10NetTo12Net

Enter number of the profile for this policy [1]? 0
Enter a Name (1-29 characters) for this Profile []? trafficFrom11NetTo13Net
Source Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]?
Enter IPV4 Source Address [0.0.0.0]? 11.0.0.0
Enter IPV4 Source Mask [255.0.0.0]?
Destination Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]?
Enter IPV4 Destination Address [0.0.0.0]? 13.0.0.0
Enter IPV4 Destination Mask [255.0.0.0]?

Protocol IDs:
  1) TCP
  2) UDP
  3) All Protocols
  4) Specify Range

Select the protocol to filter on (1-4) [3]? 1
Enter the Starting value for the Source Port [0]?
Enter the Ending value for the Source Port [65535]?
Enter the Starting value for the Destination Port [0]?
Enter the Ending value for the Destination Port [65535]?
Enter the Mask to be applied to the Received DS-byte [0]?
Enter the value to match against after the Mask has
been applied to the Received DS-byte [0]?
Configure local and remote ID's for ISAKMP? [No]:
Limit this profile to specific interface(s)? [No]:

Here is the Profile you specified...

Profile Name      = trafficFrom11NetTo13Net
sAddr:Mask=      11.0.0.0 : 255.0.0.0      sPort=   0 : 65535
dAddr:Mask=      13.0.0.0 : 255.0.0.0      dPort=   0 : 65535
proto            =                6 : 6
TOS              =                x00 : x00
Remote Grp=All Users

Is this correct? [Yes]:
List of Profiles:
  0: New Profile
  1: trafficFrom10NetTo12Net
  2: trafficFrom11NetTo13Net

Enter number of the profile for this policy [1]? 2
```

2. Vuelva a utilizar el período de validez.

List of Validity Periods:

- 0: New Validity Period
- 1: MonToFri-9am:5pm-1999

Enter number of the validity period for this policy [1]?

Should this policy enforce an IPSEC action? [No]: **yes**

IPSEC Actions:

- 0: New IPSEC Action
- 1: secure11NetTo12Net

Enter the Number of the IPSEC Action [1]? **0**

Enter a Name (1-29 characters) for this IPsec Action []? **secure11To13**

List of IPsec Security Action types:

- 1) Block (block connection)
- 2) Permit

Select the Security Action type (1-2) [2]?

Should the traffic flow into a secure tunnel or in the clear:

- 1) Clear
- 2) Secure Tunnel

[2]?

Enter Tunnel Start Point IPV4 Address

[11.0.0.5]? **1.1.1.1**

Enter Tunnel End Point IPV4 Address (0.0.0.0 for Remote Access)

[0.0.0.0]? **1.1.1.3**

Does this IPSEC tunnel flow within another IPSEC tunnel? [No]:

Percentage of SA lifesize/lifetime to use as the acceptable minimum [75]?

Security Association Refresh Threshold, in percent (1-100) [85]?

Options for DF Bit in outer header (tunnel mode):

- 1) Copy
- 2) Set
- 3) Clear

Enter choice (1-3) [1]?

Enable Replay prevention (1=enable, 2=disable) [2]?

Do you want to negotiate the security association at

system initialization(Y-N)? [No]:

You must choose the proposals to be sent/checked against during phase 2 negotiations. Proposals should be entered in order of priority.

3. Vuelva a utilizar la propuesta de IPSec de la configuración definida anteriormente.

Utilización de la característica de política

List of IPSEC Proposals:

0: New Proposal
1: genP2Proposal

Enter the Number of the IPSEC Proposal [1]?

Are there any more Proposal definitions for this IPSEC Action? [No]:

Here is the IPsec Action you specified...

```
IPSECAction Name = secure11To13
  Tunnel Start:End      =      1.1.1.1 : 1.1.1.3
  Tunnel In Tunnel      =      No
  Min Percent of SA Life =      75
  Refresh Threshold     =      85 %
  Autostart             =      No
  DF Bit                =      COPY
  Replay Prevention     =      Disabled
  IPSEC Proposals:
    genP2Proposal
Is this correct? [Yes]:
IPSEC Actions:
  0: New IPSEC Action
  1: secure11NetTo12Net
  2: secure11To13
```

Enter the Number of the IPSEC Action [1]? 2

4. Vuelva a utilizar la acción de ISAKMP de la configuración anterior.

```
ISAKMP Actions:
  0: New ISAKMP Action
  1: genPhase1Action
```

Enter the Number of the ISAKMP Action [1]?

Do you wish to Map a DiffServ Action to this Policy? [No]:

Policy Enabled/Disabled (1. Enabled, 2. Disabled) [1]?

Here is the Policy you specified...

```
Policy Name      = examplePolicySecure11to13
  State:Priority =Enabled   : 10
  Profile        =trafficFrom11NetTo13Net
  Valid Period   =MonToFri-9am:5pm-1999
  IPSEC Action   =secure11To13
  ISAKMP Action  =genPhase1Action
```

Is this correct? [Yes]:

Eliminar todo el tráfico público (regla de filtro)

Este ejemplo de política muestra cómo configurar una regla de eliminación sencilla para la interfaz pública, que elimina todo el tráfico que no está asegurado mediante IPsec. Esta regla es muy general y **debe** tener la prioridad más baja de todas las reglas configuradas.

1. Añada la política.

```

Policy config>add policy
Enter a Name (1-29 characters) for this Policy []? dropAllPublicTraffic
Enter the priority of this policy (This number is used to
determine the policy to enforce in the event of policy conflicts) [5]?
List of Profiles:
  0: New Profile
  1: trafficFrom10NetTo12Net
  2: trafficFrom11NetTo13Net

Enter number of the profile for this policy [1]? 0
  
```

2. Defina un perfil nuevo que incluya todo el tráfico que entra y sale de la interfaz pública (1.1.1.1).

```

Enter a Name (1-29 characters) for this Profile []? allPublicTraffic
Source Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]?
Enter IPV4 Source Address [0.0.0.0]?
Enter IPV4 Source Mask [0.0.0.0]?
Destination Address Format (1:NetMask, 2:Range, 3:Single Addr) [1]?
Enter IPV4 Destination Address [0.0.0.0]?
Enter IPV4 Destination Mask [0.0.0.0]?

Protocol IDs:
  1) TCP
  2) UDP
  3) All Protocols
  4) Specify Range

Select the protocol to filter on (1-4) [3]?
Enter the Starting value for the Source Port [0]?
Enter the Ending value for the Source Port [65535]?
Enter the Starting value for the Destination Port [0]?
Enter the Ending value for the Destination Port [65535]?
Enter the Mask to be applied to the Received DS-byte [0]?
Enter the value to match against after the Mask has
been applied to the Received DS-byte [0]?
Configure local and remote ID's for ISAKMP? [No]:
  
```

3. Dado que la información de origen y de destino (o ambas) contenía caracteres comodines, debe especificar las interfaces en las que espera que este tráfico entre y salga.

```

The Source and/or Destination Address information you specified
includes all addresses. You must specify an Interface Pair
with this profile to further qualify what traffic you wish to filter
to this policy. The interface pair should at least specify the
Limit this profile to specific interface(s)? [No]: yes
Interface Pair Groups:
  0: New Ifc Pair
Number of Ifc Pair Group [1]? 0
  
```

4. Añada una interfaz pareja para el tráfico que sale a través de la interfaz pública.

Utilización de la característica de política

```
Enter a Group Name (1-29 characters) for this Interface Pair []? inOutPublic
Ingress Interface IP Address (255.255.255.255 = any ingress)
[255.255.255.255]?
Egress Interface IP Address (255.255.255.255 = any egress)
[255.255.255.255]? 1.1.1.1
Interface Pair Groups:
  0: New Ifc Pair
  1) Group Name: inOutPublic
     In:Out=255.255.255.255 : 1.1.1.1

Number of Ifc Pair Group [1]? 0
```

5. Añada otra interfaz pareja para el tráfico que entra a través de la interfaz pública. Dele el mismo nombre que a la interfaz pareja anterior para asignarla al mismo grupo.

```
Enter a Group Name (1-29 characters) for this Interface Pair []? inOutPublic
Ingress Interface IP Address (255.255.255.255 = any ingress)
[255.255.255.255]? 1.1.1.1
Egress Interface IP Address (255.255.255.255 = any egress)
[255.255.255.255]?
Interface Pair Groups:
  0: New Ifc Pair
  1) Group Name: inOutPublic
     In:Out=255.255.255.255 : 1.1.1.1
     In:Out= 1.1.1.1 : 255.255.255.255

Number of Ifc Pair Group [1]?
```

Here is the Profile you specified...

```
Profile Name = allPublicTraffic
sAddr:Mask= 0.0.0.0 : 0.0.0.0      sPort= 0 : 65535
dAddr:Mask= 0.0.0.0 : 0.0.0.0      dPort= 0 : 65535
proto = 0 : 255
TOS = x00 : x00
Remote Grp=All Users
1. In:Out=255.255.255.255 : 1.1.1.1
2. In:Out= 1.1.1.1 : 255.255.255.255

Is this correct? [Yes]:
List of Profiles:
  0: New Profile
  1: trafficFrom10NetTo12Net
  2: trafficFrom11NetTo13Net
  3: allPublicTraffic

Enter number of the profile for this policy [1]? 3
```

6. Añada un nuevo período de validez que especifique all the time (todo el tiempo).

List of Validity Periods:

- 0: New Validity Period
- 1: MonToFri-9am:5pm-1999

Enter number of the validity period for this policy [1]? **0**

Enter a Name (1-29 characters) for this Policy Valid Profile []? **allTheTime**

Enter the lifetime of this policy. Please input the information in the following format:

yyyymmddhhmmss:yyyymmddhhmmss OR '*' denotes forever.

[*]?

During which months should policies containing this profile be valid. Please input any sequence of months by typing in the first three letters of each month with a space in between each entry, or type ALL to signify year round.

[ALL]?

During which days should policies containing this profile be valid. Please input any sequence of days by typing in the first three letters of each day with a space in between each entry, or type ALL to signify all week

[ALL]?

Enter the starting time (hh:mm:ss or * denotes all day)

[*]?

Here is the Policy Validity Profile you specified...

```
Validity Name = allTheTime
Duration     = Forever
Months      = ALL
Days        = ALL
Hours       = All Day
```

Is this correct? [Yes]:

List of Validity Periods:

- 0: New Validity Period
- 1: MonToFri-9am:5pm-1999
- 2: allTheTime

Enter number of the validity period for this policy [1]? **2**

Should this policy enforce an IPSEC action? [No]: **yes**

IPSEC Actions:

- 0: New IPSEC Action
- 1: secure11NetTo12Net
- 2: secure11To13

7. Añada una nueva acción de IPSec para eliminar todo el tráfico (acción de filtro).

Utilización de la característica de política

```
Enter the Number of the IPSEC Action [1]? 0
Enter a Name (1-29 characters) for this IPsec Action []? dropTraffic
List of IPsec Security Action types:
  1) Block (block connection)
  2) Permit

Select the Security Action type (1-2) [2]? 1

Here is the IPsec Action you specified...

IPSECAction Name = dropTraffic
  Action = Drop
Is this correct? [Yes]:
IPSEC Actions:
  0: New IPSEC Action
  1: secure11NetTo12Net
  2: secure11To13
  3: dropTraffic

Enter the Number of the IPSEC Action [1]? 3
Do you wish to Map a DiffServ Action to this Policy? [No]:
Policy Enabled/Disabled (1. Enabled, 2. Disabled) [1]?

Here is the Policy you specified...

Policy Name      = dropAllPublicTraffic
  State:Priority =Enabled   : 5
  Profile        =allPublicTraffic
  Valid Period   =allTheTime
  IPSEC Action   =dropTraffic
Is this correct? [Yes]:
```

Configuración y habilitación del motor de búsqueda de política LDAP

Este ejemplo muestra cómo configurar y habilitar el motor de búsqueda de política LDAP. En este ejemplo, hay dos directorios de LDAP (uno primario y otro secundario) con las direcciones IP 11.0.0.2 y 13.0.0.1, respectivamente. Ambas escuchan en el puerto TCP 389 y el dispositivo se debe vincular al servidor LDAP como cn=router, contraseña myPassWord. La entrada base en el árbol de directorios para las políticas del direccionador es cn=RouterDeviceProfile,o=ibm,c=us.

Nota: Actualmente, tanto el servidor LDAP primario como el secundario deben estar escuchando en el mismo puerto y tener las mismas credenciales de autenticación para el direccionador. DeviceProfile debe ser el mismo para el direccionador en ambos servidores de directorios.

Este ejemplo muestra también cómo definir la política por omisión, de manera que las comunicaciones LDAP estén aseguradas a través de IPsec. Este ejemplo utiliza la clave precompartida para la autenticación ISAKMP, y SHA y 3DES para los parámetros de autenticación y cifrado para las fases 1 y 2. El punto inicial del túnel es 1.1.1.4 para el dispositivo que ejecuta la búsqueda de política LDAP y los puntos finales del túnel son 1.1.1.1 para el servidor LDAP 11.0.0.1, y 1.1.1.3 para el servidor LDAP 13.0.0.1 .

1. Configure y habilite el motor de búsqueda de política LDAP y liste los resultados.

```
Policy config>set ldap primary-server 11.0.0.1
Policy config>set ldap secondary-server 13.0.0.1
Policy config>set ldap port 389
Policy config>set ldap bind-name cn=router
Policy config>set ldap bind-pw myPassWord
Policy config>set ldap anonymous-bind no
Policy config>set ldap policy-base cn=RouterDeviceProfile,o=ibm,c=us
Policy config>enable ldap policy-search
Policy config>list ldap
LDAP CONFIGURATION information:

      Primary Server Address:          11.0.0.1
      Secondary Server Address:       13.0.0.1

      Search timeout value:           3 sec(s)
      Retry interval on search failures: 1 min(s)
      Server TCP port number:         389
      Server Version number:          2

      Bind Information:
      Bind Anonymously:                No
      Device Distinguished Name:       cn=router
      Device Password:                 myPassWord

      Base DN for this device's policies: cn=RouterDeviceProfile,o=ibm,c=us

      Search policies from LDAP Directory: Enabled
```

2. Defina la política por omisión

Utilización de la característica de política

```
Policy config>set default-policy
List of default policy rules:
  1) Accept and Forward all IP Traffic
  2) Permit LDAP traffic, drop all other IP Traffic
  3) Permit and Secure LDAP traffic, drop all other IP Traffic

Select the default policy rule to use during policy refresh periods [1]? 3
List of default error handling procedures:
  1) Reset Policy Database to Default Rule
  2) Flush any rules read from LDAP, load local rules

Select the error handling behavior for when loading Policy Database [1]?

Please enter the set of Security Information for encrypting and
authenticating the LDAP traffic generated by the device when
retrieving policy information from the LDAP Server

Enter phase 1 ISAKMP negotiation parameters:

List of Diffie Hellman Groups:
  1) Diffie Hellman Group 1
  2) Diffie Hellman Group 2

Select the Diffie Hellman Group ID from this proposal (1-2) [1]?

List of Hashing Algorithms:
  1) MD5
  2) SHA

Select the hashing algorithm(1-2) [1]? 2

List of Cipher Algorithms:
  1) DES
  2) 3DES

Select the Cipher Algorithm (1-2) [1]? 2
Authentication: (1)Pre-shared Key or (2)Certificate(RSA Sig) [2]? 1
Enter the Pre-Shared Key []? test

Enter phase 2 IPSEC negotiation parameters:
List of IPsec Authentication Algorithms:
  0) None
  1) HMAC-MD5
  2) HMAC_SHA

Select the ESP Authentication Algorithm (0-2) [1]? 2
List of ESP Cipher Algorithms:
  1) ESP DES
  2) ESP 3DES
  3) ESP CDMF
  4) ESP NULL

Select the ESP Cipher Algorithm (1-4) [1]? 2
Tunnel Start IPV4 Address (Primary LDAP Server)
[0.0.0.0]? 1.1.1.4
Tunnel End Point IPV4 Address (Primary LDAP Server)
[0.0.0.0]? 1.1.1.1
Tunnel Start IPV4 Address (Secondary LDAP Server)
[1.1.1.4]?
Tunnel End Point IPV4 Address (Secondary LDAP Server)
[1.1.1.1]? 1.1.1.3
Policy config>list default-policy

Default Policy Rule:                Drop All IP Traffic except secure LDAP
Default error handling procedure:    Reset Policy Database to Default Rule

Phase 1 ISAKMP negotiation parameters:
Diffie Hellman Group ID:            1
Hashing Algorithm:                  SHA
ISAKMP Cipher Algorithm:            ESP 3DES CBC
Per-shared key value:               test
```



```
Phase 2 IPSEC negotiation parameters:  
IPsec ESP Authentication Algorithm:  HMAC SHA  
ESP Cipher Algorithm:                3DES  
Local Tunnel Addr (Primary Server):  1.1.1.4  
Remote Tunnel Addr (Primary Server):  1.1.1.1  
Local Tunnel Addr (Secondary Server): 1.1.1.4  
Remote Tunnel Addr (Secondary Server): 1.1.1.3
```

En estos momentos, está preparado para gestionar los direccionadores de la red con la característica de política. Para obtener información detallada acerca de los mandatos que se utilizan para configurar los parámetros de política obligatorios, tales como los perfiles, las propuestas, las transformaciones y las acciones, consulte las secciones “Mandatos de configuración de política” en la página 343, “Mandatos de configuración del servidor de política LDAP” en la página 358 y “Mandatos de supervisión de política” en la página 363.

Utilización de la característica de política

Configuración y supervisión de la característica de política

Este capítulo describe los mandatos de LDAP y de política proporcionados por la característica de política para configurar y operar los dispositivos direccionadores en una red. Incluye las secciones siguientes:

- “Acceso al indicador de configuración de política”
- “Mandatos de configuración de política”
- “Mandatos de configuración del servidor de política LDAP” en la página 358
- “Acceso al indicador de supervisión de política” en la página 363
- “Mandatos de supervisión de política” en la página 363

Acceso al indicador de configuración de política

Para entrar mandatos de configuración de política:

1. Entre **talk 6** en el indicador OPCON (*).
2. Entre **feature policy** en el indicador Config>.

Aparece el indicador Policy config>. Ahora puede entrar los mandatos de configuración de política.

Mandatos de configuración de política

Estos mandatos le permiten configurar la información contenida en las políticas. La Tabla 44 resume los mandatos de configuración de política y el resto de esta sección los describe de manera detallada. Entre estos mandatos en el indicador Policy config>. Puede entrar el mandato y las opciones en una línea, o entrar únicamente el mandato y responder a las solicitudes. Para ver una lista de las opciones de mandato válidas, entre el mandato con un signo de interrogación en lugar de especificar opciones.

Tabla 44. Mandatos de configuración de política

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxiv.
Add	Añade la información utilizada para crear una política.
Change	Cambia la información que compone una política.
Copy	Copia información de una política a otra.
Delete	Suprime información de una política.
Disable	Inhabilita una política.
Enable	Habilita una política.
List	Visualiza la información en una política.
Set	Especifica una política que va a utilizarse como política por omisión.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiv.

Add

Utilice el mandato **add** para añadir información a una política.

Sintaxis: add diffserv-action
 interface-pair
 ipsec-action
 ipsec-manual-tunn
 ipsec-proposal
 ipsec-transform
 isakmp-action
 isakmp-proposal
 policy
 profile
 rsvp-action
 user
 validity-period

Diffserv-action

Solicita información acerca de las selecciones de acción de DiffServ que se quieren aplicar.

name

Nombre exclusivo de la acción de DiffServ para la política.

permission-level

Especifica si el direccionador va a reenviar los paquetes que coincidan con esta acción de DiffServ.

1

Permitir

2

Denegar

Valor por omisión: 2

queue-priority

Cola en la que se colocan los paquetes de salida que coinciden con esta acción de DiffServ.

1

Calidad superior (reenvío urgente)

2

Asegurado/Mejor esfuerzo

Valor por omisión: 2

bwshare-type

Tipo de asignación de compartición del ancho de banda.

1

Absoluto (en Kbps)

2

Porcentaje (de ancho de banda de salida total)

Valor por omisión: 2

bwshare

Ancho de banda (en Kbps o como porcentaje del ancho de banda de salida) asignado a este servicio.

ds-bytemask

Máscara que se aplicará a los bytes de ds transmitidos. Este valor designa qué bits del byte TOS de un paquete se deben modificar cuando se transmite el paquete. Un cero en cualquier posición de bit de este byte implica que el bit no debe modificarse.

Valor por omisión:

00

(no cambie ningún bit)

ds-bytemodify

El marcado del byte TOS de IP que debe aplicarse a los paquetes que serán reenviados por este dispositivo. Los ceros incluidos en la máscara implican que el bit correspondiente no se modificará. Un uno implica que el bit se marcará con el valor de bit en el byte de la marca. La operación es: $\text{newTOSByte} = (\text{Mask} \& \text{receivedTOSByte}) | (\text{Mask} \& \text{Mark})$ El signo \wedge es un complemento basado en bits (Mask:Mark)

Ejemplo:

11111101:00000001

Mediante este ejemplo, el valor 0x07 recibido se enviaría con el valor 0x03

Valor por omisión: X'00' (no cambiar ningún bit)

interface-pair

El par de interfaces asocia un perfil con una interfaz o un conjunto de interfaces determinado. Por omisión, el objeto de perfil no limita que se aplique la política a ninguna interfaz. Si es necesario, puede añadir pares de interfaces para conseguirlo. El par de interfaces especifica la dirección IP de la interfaz a la que debe llegar el tráfico y la dirección IP de la interfaz por la que debe salir.

El ejemplo siguiente muestra dos pares de interfaces que tienen el mismo nombre y que representan el tráfico que llega a una interfaz cualquiera y sale por la interfaz pública, y viceversa.

```
1) Group Name: inOutPublic
   In:Out=255.255.255.255 : 1.1.1.1
   In:Out=1.1.1.1 : 255.255.255.255
```

Name

Nombre del par de interfaces.

Ingress interface

Dirección IPv4 de la interfaz de entrada.

Valor por omisión: 255.255.255.255 (cualquiera)

Egress interface

Dirección IPv4 de la interfaz de salida.

Valor por omisión: 255.255.255.255 (cualquiera)

IPSec-action

Solicita información para configurar el túnel de fase 2.

Mandatos de configuración de política (Talk 6)

Name

Nombre de la acción de IPSec.

Action type

Acción que se debe aplicar a los paquetes que coincidan con el perfil de una política que contiene esta acción.

- 1 Bloque (conexión de bloque).
- 2 Permitir (Permitir los paquetes que coincidan con esta acción.) Si una propuesta de IPSec no existe, se pasa el paquete; si existe, se aplica el proceso de seguridad de IPSec al paquete.

Valor por omisión: 2

La siguiente opción sólo está disponible si se especifica pasar como tipo de acción:

Traffic flow type

Tipo de flujo de tráfico (túnel seguro o al descubierto).

- 1 Al descubierto
- 2 Túnel seguro

Valor por omisión: 2

La siguiente opción sólo está disponible si se especifica el flujo de tráfico seguro:

Tunnel start point

Dirección IPv4 del punto inicial del túnel.

Tunnel end point

Dirección IPv4 del punto final del túnel. (0.0.0.0 para el acceso remoto)

Valor por omisión: 0.0.0.0

Tunnel-in-tunnel

Especifica si el tráfico protegido por este túnel debe seguir protegido además por otra política configurada en este dispositivo.

Opciones válidas: Yes o No

Valor por omisión: No

Percentage of SA lifiesize/lifetime to accept

Tamaño y tiempo de duración mínimos de SA (como porcentaje). No se aceptará un valor de tamaño y tiempo de duración de SA recibido que sea menor que éste.

Valor por omisión: 75

SA refresh threshold

Porcentaje del tiempo o tamaño de duración de SA en el cual la SA debe renovarse automáticamente.

Valor por omisión: 85

DF-Bit-Setting

Especifica si se debe copiar el bit DF (No fragmentar) desde el paquete original, y si se debe definir o borrar en la cabecera externa del paquete de IPSec si se ejecuta en la modalidad de túnel.

- 1 Copiar
- 2 Definir
- 3 Borrar

Valor por omisión: 1

Replay-Prevention

Especifica si IPSec debe aplicar la prevención de reproducción en los paquetes de IPSec recibidos. En esta modalidad, IPSec asegura que los números de secuencia son válidos y no se reciben más de una vez.

- 1 Habilitar
- 2 Inhabilitar

Valor por omisión: 2

Negotiate SA Automatically

Especifica si la SA de fase 2 se negocia automáticamente en la inicialización del sistema.

Yes o No

Valor por omisión: No

IPSec proposal

El nombre de la propuesta de IPSec (puede especificar un máximo de cinco propuestas) que se debe enviar o comprobar durante la fase 2. El orden en que las especifique determinará su prioridad, siendo la primera la de prioridad más alta.

IPSec-manual-tunn

Solicita información para configurar manualmente el túnel de fase 2.

Tunnel name

Nombre del túnel manual de IPSec.

Tunnel lifetime

Duración del túnel (en minutos).

Valor por omisión: 46080

Encapsulation mode

Modalidad de encapsulación que se va a utilizar.

tunn

Modalidad de túnel

trans

Modalidad de transporte

Valor por omisión: tunn

Mandatos de configuración de política (Talk 6)

Policy

Tipo de política de túnel que se va a utilizar.

AH

Cabecera de autenticación

ESP

Carga de seguridad de encapsulación

AH-ESP

Para los paquetes de salida, especifica que se ejecuta el cifrado antes que la autenticación.

ESP-AH

Para los paquetes de salida, especifica que se ejecuta la autenticación antes que el cifrado.

Valor por omisión: AH-ESP

Local IP address

Dirección IPv4 de origen.

Valor por omisión: 11.0.0.5

Local encryption SPI

Valor de índice de parámetros de seguridad de origen.

Valor por omisión: 256

Local encryption algorithm

Algoritmo de cifrado de origen.

Null

Sin cifrado.

CDMF

Commercial Data Masking Facility (Recurso de enmascaramiento de datos comerciales).

DES-CBC

Data Encryption Standard (Estándar de cifrado de datos) y Cipher Block Chaining (Encadenado de bloques de cifrado).

3DES

Triple Data Encryption Standard (Estándar de triple cifrado de datos).

Valor por omisión: DES-CBC

Local encryption key

Una clave de 16 caracteres.

Padding

Relleno adicional para el cifrado local.

Valor por omisión: 0

Local ESP authentication

Especifica si se debe utilizar la autenticación de ESP local.

Yes o No

Valor por omisión: Yes

Remote IP address

Dirección IPv4 de destino.

Valor por omisión: 0.0.0.0

Remote encryption SPI

Valor de índice de parámetros de seguridad de destino.

Valor por omisión: 256

Remote encryption algorithm

El algoritmo de cifrado de destino.

Null

Sin cifrado.

CDMF

Commercial Data Masking Facility (Recurso de enmascaramiento de datos comerciales).

DES-CBC

Data Encryption Standard (Estándar de cifrado de datos) y Cipher Block Chaining (Encadenado de bloques de cifrado).

3DES

Triple Data Encryption Standard (Estándar de triple cifrado de datos).

Valor por omisión: DES-CBC

Remote encryption key

Una clave de 16 caracteres.

Verify remote encryption padding.

Especifica si se verifica o no el relleno de cifrado.

Yes o No

Valor por omisión: No

Remote ESP authentication

Especifica si se debe utilizar la autenticación de ESP remota.

Yes o No

Valor por omisión: Yes

DF bit

Especifica cómo procesar el bit DF (No fragmentar).

Copy

Copia el bit DF.

Set

Activa el bit DF.

Clear

Desactiva el bit DF.

Valor por omisión: COPY

Enable tunnel

Especifica si se habilita o no el túnel al crearlo.

Mandatos de configuración de política (Talk 6)

Yes o No

Valor por omisión: Yes

IPSec-proposal

Solicita información para crear una propuesta de IPSec.

IPSec proposal name

Nombre de la propuesta de IPSec.

Perfect forward secrecy

Especifica si se debe utilizar IKE, para evitar que alguien determine una clave actual a partir de una clave comprometida anteriormente.

Yes o No

Valor por omisión: No

Diffie Hellman Group ID

Tipo de grupo Diffie Hellman.

1

Grupo 1 de Diffie Hellman

2

Grupo 2 de Diffie Hellman

Valor por omisión: 1

AH transform

Nombre de la transformación de la AH (puede especificar un máximo de cinco transformaciones) para esta propuesta. El orden en que las especifique determinará su prioridad, siendo la primera la de prioridad más alta.

ESP transform

Nombre de la transformación de la ESP (puede especificar un máximo de cinco propuestas) para esta propuesta. El orden en que las especifique determinará su prioridad, siendo la primera la de prioridad más alta.

IPSec-transform

Solicita información acerca de las transformaciones de IPSec.

IPSec transform name

Nombre de la transformación de IPSec.

Protocol ID

Protocolo de seguridad que se va a utilizar.

1

IPSec-AH

2

IPSec-ESP

Valor por omisión: 1

AH Authentication Algorithm

Algoritmo de autenticación de AH que se va a utilizar.

1

HMAC-MD5

2
HMAC-SHA

Valor por omisión: 1

Encapsulation mode

Modalidad de encapsulación que se va a utilizar.

1
Túnel

2
Transporte

Valor por omisión: 1

ESP Authentication Algorithm

Algoritmo de autenticación de ESP que se va a utilizar.

0
Ninguno

1
HMAC-MD5

2
HMAC-SHA

Valor por omisión: 2

ESP cipher algorithm

Algoritmo de cifrado de ESP que se va a utilizar.

1
ESP DES

2
ESP 3DES

3
ESP CDMF

4
ESP Null (sin cifrado)

Valor por omisión: 1

SA lifesize

Tamaño (en Kb) de la SA para esta propuesta.

Valor por omisión: 50000

SA lifetime

Duración (en segundos) de la SA para esta propuesta.

Valor por omisión: 3600

ISAKMP-Action

Solicita información acerca de la acción de ISAKMP que se aplica.

Name

Nombre de la acción de ISAKMP.

Exchange mode

Tipo de modalidad de intercambio de las negociaciones de fase 1.

Mandatos de configuración de política (Talk 6)

1
Principal

2
Agresiva

Valor por omisión: 1

Percentage of Minimum SA lifiesize/lifetime

Tamaño y tiempo de duración mínimos de SA (como porcentaje). No se aceptará un valor de tamaño y tiempo de duración de SA que sea menor que éste.

Valor por omisión: 75

ISAKMP connection lifiesize

Tamaño (en Kb) de la conexión de fase 1. Una vez que haya caducado la conexión de la fase 1, la vez siguiente que se deba renovar la SA de la fase 2, la fase 1 se renegociará por completo antes de que la fase 2 pueda empezar.

Valor por omisión: 5000

ISAKMP connection lifetime

Duración (en segundos) de la conexión de la fase 1. Una vez que haya caducado la conexión de la fase 1, la vez siguiente que se deba renovar la fase 2, la fase 1 se reiniciará por completo.

Valor por omisión: 5000

Negotiate SA automatically

Especifica si la SA se negociará automáticamente en la inicialización del sistema.

Yes o No

Valor por omisión: No

ISAKMP proposal

El nombre de la propuesta de ISAKMP (puede especificar un máximo de cinco propuestas) que se debe enviar o comprobar durante la modalidad rápida de la fase 2. El orden en que las especifique determinará su prioridad, siendo la primera la de prioridad más alta.

ISAKMP-Proposal

Solicita la información de propuesta de ISAKMP utilizada en las negociaciones de ISAKMP.

ISAKMP proposal name

Nombre de la propuesta de ISAKMP.

Authentication method

Tipo de autenticación que se va a utilizar durante las negociaciones de la fase 1 de ISAKMP.

1
Clave precompartida

2
RSA SIG (modalidad de certificación)

Valor por omisión: 1

Hash algorithm

Tipo de algoritmo hash que se va a utilizar durante las negociaciones de la fase 1.

- 1
MD5
- 2
SHA

Valor por omisión: 1

Cipher algorithm

Tipo de algoritmo de cifras que se va a utilizar durante las negociaciones de la fase 1.

- 1
DES
- 2
3DES

Valor por omisión: 1

Diffie Hellman Group ID

Tipo de grupo Diffie Hellman que se va a utilizar durante las negociaciones de la fase 1.

- 1
Grupo 1 de Diffie Hellman
- 2
Grupo 2 de Diffie Hellman

Valor por omisión: 1

SA lifesize

Tamaño (en Kb) de la SA para esta propuesta.

Valor por omisión: 50000

SA lifetime

Duración (en segundos) de la SA para esta propuesta.

Valor por omisión: 5000

Policy

Solicita información acerca de la configuración de política: Nombre de perfil (obligatorio), nombre de RSVP (opcional), nombre de DiffServ (opcional), nombre de IPSec (opcional), nombre de ISAKMP (opcional) y perfil de período de validez (opcional). Debe especificar DiffServ, IPSec, ISAKMP o RSVP para que la política sea válida.

Valor por omisión: Siempre válido

Name Nombre de la configuración de política

Priority Prioridad relativa de esta política respecto a otras (cuanto mayor sea el número, más alta es la prioridad). Se utiliza para resolver conflictos si varias políticas son aplicables a un paquete.

Valor por omisión: 5

Profile Nombre de un perfil de tráfico de datos configurado anteriormente que se va a utilizar para esta política.

Mandatos de configuración de política (Talk 6)

Validity period Nombre de un período de validez configurado anteriormente que se va a utilizar para esta política.

IPSec action Si esta política aplicará una acción de IPSec, nombre de una acción de IPSec configurada anteriormente que se va a utilizar para esta política. Si especifica una acción de IPSec segura, debe especificar también una acción de ISAKMP.

ISAKMP action Nombre de una acción de ISAKMP configurada anteriormente que se va a utilizar para esta política. Si especifica una acción de ISAKMP, debe especificar también una acción de IPSec.

Diffserv action Si desea correlacionar una acción de DiffServ con esta política, es el nombre de una acción de DiffServ configurada anteriormente.

RSVP action Nombre de una acción de RSVP que esta política debe aplicar.

Profile

Solicita información para definir un conjunto de selectores (condicionales) para un perfil de política en el que se ejecutarán acciones.

name

Nombre del perfil de política

ipv4-src-address-format

Formato de la dirección IPv4 de origen (rango, máscara de red, dirección única).

ipv4-src-address

Dirección IPv4 de origen (dirección baja, si el formato de dirección es *range*).

Valor por omisión: 0.0.0.0

ipv4-src-mask

Máscara IPv4 de origen (dirección alta, si el formato de dirección es *range*).

Valor por omisión: 255.0.0.0

ipv4-dest-address-format

Formato de la dirección IPv4 de destino (rango, máscara de red, dirección única).

ipv4-dest-address

Dirección IPv4 de destino (dirección baja, si el formato de dirección es *range*).

Valor por omisión: 0.0.0.0

ipv4-dest-mask

Máscara IPv4 de destino (dirección alta, si el formato de dirección es *range*).

Valor por omisión: 255.0.0.0

protocol-id

ID de protocolo en el que se realiza el filtrado.

1

TCP

2
UDP

3
Todos los protocolos

4
Especificar rango

Valor por omisión: 3

src-port-start

Primer número de puerto del rango de números de puerto de origen.

Valor por omisión: 0

src-port-end

Último número de puerto del rango de números de puerto de origen.

Valor por omisión: 65535

dest-port-start

Primer número de puerto del rango de números de puerto de destino.

Valor por omisión: 0

dest-port-end

Último número de puerto del rango de números de puerto de destino.

Valor por omisión: 65535

src-id-type

Tipo de ID de origen que se envía al remoto. Este valor se utiliza para determinar cuál es la política que contiene la información de ISAKMP necesaria durante las negociaciones de la fase 1 de ISAKMP. Se compara con la información de la carga de identificación del paquete ISAKMP. Esta información es necesaria, si el similar remoto debe identificar el dispositivo con un valor distinto de la dirección IP.

1
Punto final de túnel local

2
Nombre de dominio de sistema principal calificado al completo

3
Nombre de dominio de usuario calificado al completo

4
ID de clave

any-user-access

Permite el acceso para cualquier usuario incluido en la definición de perfil. Si especifica No, se le solicitará el nombre del grupo de usuarios remotos para este perfil. Este atributo sólo es obligatorio si desea limitar el acceso de los similares de acceso remoto a una política específica.

Yes o No

Valor por omisión: Yes

Received DS byte mask

Máscara de 8 bits que se debe aplicar al byte TOS de un paquete de entrada.

Mandatos de configuración de política (Talk 6)

Valor por omisión: 0

Received DS byte match

Patrón de 8 bits para comparar con el resultado de AND en el byte TOS de entrada con el valor de máscara de byte DS recibido.

Valor por omisión: 0

Interface pairs

Si esta política debe restringir los flujos de tráfico a unas interfaces específicas, éste es el nombre del grupo de pares de interfaces.

RSVP-Action

Solicita información acerca de cuáles son las acciones de RSVP que se aplican.

Name

Nombre de la acción de RSVP.

Permission

Especifica el nivel de permiso para las sesiones de RSVP que coincidan con esta acción.

1

Permitir

2

Denegar

Valor por omisión: 2

Max token rate

Cantidad máxima de ancho de banda (en Kbps) que RSVP va a asignar para un flujo individual.

Valor por omisión: 100

Max duration

Cantidad máxima de tiempo (en segundos) que puede durar un flujo (0 implica una duración ilimitada).

Valor por omisión: 600

RSVP-to-DS

Especifica si se correlacionan los flujos de RSVP que corresponden a esta acción con una acción de DiffServ configurada. RSVP utiliza la información de la acción de DiffServ para marcar el byte TOS para el siguiente dispositivo de ascenso habilitado por DiffServ. Deberá utilizarse en una red en la que los paquetes salgan de una red habilitada por RSVP hacia una red habilitada por DiffServ.

Yes o No

Valor por omisión: No

VALIDITY-PERIOD

Le solicita información acerca del período durante el cual la política es válida, y crea un perfil de política.

Name

Nombre del perfil del período de validez.

yyyymmddhhmmss:yyyymmddhhmmss

Período durante el cual las políticas que contienen este perfil de período de validez son válidas.

Ejemplo:

19980101000000:19981231000000

Months

Meses durante los cuales las políticas que contienen este perfil de período de validez son válidas. Puede especificar cualquier secuencia de meses, empleando las tres primeras letras de cada mes en inglés (por ejemplo, JAN para enero, DEC para diciembre, etc.), con los meses separados por un espacio, o bien puede especificar a11 (todos) para indicar todos los meses del año.

Days

Fechas durante las cuales las políticas que contienen este perfil de período de validez son válidas. Puede especificar cualquier secuencia de fechas, empleando las tres primeras letras de cada día en inglés (por ejemplo, MON para lunes, FRI para viernes, etc.), con los días separados por un espacio, o bien puede entrar a11 (todos) para indicar todos los días de la semana.

Starting time

Hora a la que las políticas que contienen este perfil de período de validez son válidas. Especifíquela con el formato hh:mm:ss, o especifique * si desea que la política sea válida durante todo el día.

Valor por omisión: *

Ending time

Hora a la que caduca la validez de las políticas que contienen este perfil de período de validez. Especifíquela con el formato hh:mm:ss.

Valor por omisión: ninguno

Change

Utilice el mandato **change** para modificar la información en un objeto de política. Vea la descripción del mandato **add** para conocer cuáles son los objetos que están disponibles.

Copy

Utilice el mandato **copy** para copiar información de un objeto de política a otro. Vea la descripción del mandato **add** para conocer cuáles son los objetos que están disponibles. (El par de interfaces, el túnel manual y las opciones de usuario no son aplicables al mandato copy).

Delete

Utilice el mandato **delete** para suprimir información de un objeto de política. Vea la descripción del mandato **add** para conocer cuáles son los objetos que están disponibles.

Mandatos de configuración de LDAP (Talk 6)

Disable

Utilice el mandato **disable** para inhabilitar una configuración de política.

Sintaxis: `disable policy`

Policy

Le solicita el nombre de la configuración de política que va a inhabilitar.

Enable

Utilice el mandato **enable** para habilitar una configuración de política.

Sintaxis: `enable policy`

Policy

Le solicita el nombre de la configuración de política que va a habilitar.

List

Utilice el mandato **list** para visualizar cualquier parte de la información de configuración de política, o toda ella.

Sintaxis: `list` `all`
 `default-policy`
 `ldap`
 `refresh`

All Visualiza toda la información sobre la configuración de política.

Default-policy

Visualiza el nombre de la política por omisión.

LDAP

Visualiza los nombres de las configuraciones LDAP definidas.

Refresh

Lista el estado de renovación de la política (Enable o Disable), así como el tiempo del intervalo de renovación.

Mandatos de configuración del servidor de política LDAP

Los mandatos de configuración del servidor de política LDAP le permiten especificar opciones de servidor LDAP para recuperar la información sobre la política. La Tabla 45 en la página 359 resume los mandatos de configuración de LDAP y el resto de esta sección los describe con detalle. Éntrelos en el indicador `Policy config>`. Puede entrar el mandato y las opciones en una línea, o entrar únicamente el mandato y responder a las solicitudes. Para ver una lista de las opciones de mandato válidas, entre el mandato con un signo de interrogación en lugar de especificar opciones.

Mandatos de configuración de LDAP (Talk 6)

Estos valores sólo son válidos si se produjo un error al construir la base de datos de políticas. Cuando se produce un error, cualquiera de estas opciones hereda la seguridad por omisión de eliminar o pasar. Si selecciona la opción 2, todo el tráfico se elimina o pasa, a menos que coincida con una política definida localmente. Si la base de datos de políticas se construye satisfactoriamente, no se utiliza esta opción.

default-security

Especifica las opciones de seguridad que se utilizarán mientras se renueva la base de datos de políticas.

Nota: Una vez que la base de datos de políticas se haya construido satisfactoriamente, el funcionamiento por omisión quedará definido como "pasar" (pass). Esto quiere decir que, si un paquete no coincide con ninguna regla de política, se pasará al descubierto. Si desea que los paquetes que no coinciden con una regla se eliminen globalmente o sólo en ciertas interfaces, debe definir una política al respecto.

1 Aceptar y reenviar todo el tráfico de IP.

2 Permitir tráfico LDAP, eliminar todo el resto de tráfico IP.

Si selecciona esta opción, se le solicitarán las direcciones IP locales en el dispositivo en el que se va a enviar o recibir el tráfico LDAP.

3 Permitir y asegurar tráfico LDAP, eliminar todo el resto de tráfico IP.

Si selecciona esta opción, se le solicitará la siguiente información:

DHGroupId

El ID de grupo Diffie-Hellman que se utilizará durante las negociaciones de fase 1 de ISAKMP.

1 Grupo DH 1.

2 Grupo DH 2.

Phase1-Hash-Algorithm

Algoritmo hash que se va a utilizar durante las negociaciones de la fase 1. El algoritmo hash proporciona la autenticación de los mensajes de la fase 1.

1 MD5.

2 SHA.

Phase1-Cipher-Algorithm

Algoritmo de cifras que se va a utilizar durante las negociaciones de la fase 1. El algoritmo de cifras proporciona protección de cifrado para las negociaciones de la fase 1.

1 DES

2 3DES

Phase1-Authentication-Method

Método de autenticación que se va a utilizar con el similar remoto. Se especifica cómo determina ISAKMP si el similar remoto es realmente el dispositivo correcto con el que debe negociar.

1 Clave precompartida

2 Certificado (RSA SIG)

Pre-Shared-Key-Value

Si ha especificado el método de autenticación de la fase 1 de clave precompartida, se le solicitará que entre el valor de clave en ASCII.

Phase2-ESP-Authentication-Algorithm

ESP es el único protocolo de IPSec permitido para la seguridad por omisión. Se le solicitará el algoritmo de autenticación que se va a utilizar durante las negociaciones de fase 2 de ISAKMP.

- 0 Ninguno
- 1 HMAC-MD5
- 2 HMAC-SHA

Phase2-ESP-Cipher-Algorithm

ESP es el único protocolo de IPSec permitido para la seguridad por omisión. Se le solicitará el algoritmo de cifrado que se va a utilizar durante las negociaciones de fase 2 de ISAKMP.

- 1 ESP DES
- 2 ESP 3DES
- 3 ESP CDMF
- 4 ESP NULL

Primary-Tunnel-Start

Dirección IP en el dispositivo que va a utilizarse para el tráfico de IKE e IPSec entre el dispositivo y la pasarela de seguridad que protege el servidor LDAP primario.

Primary-Tunnel-End

Dirección IP en la pasarela de seguridad remota, que protege el servidor LDAP primario que va a utilizarse para el tráfico de IKE e IPSec.

Secondary-Tunnel-Start

Dirección IP en el dispositivo que va a utilizarse para el tráfico de IKE e IPSec entre el dispositivo y la pasarela de seguridad que protege el servidor LDAP secundario.

Secondary-Tunnel-End

Dirección IP en la pasarela de seguridad remota, que protege el servidor LDAP secundario que va a utilizarse para el tráfico de IKE e IPSec.

Set LDAP

Utilice el mandato **set ldap** para configurar los parámetros operativos de LDAP.

Sintaxis: set ldap anonymous-bind

yes

no

bind-name <nombre>

bind-pw <contr>

policy-base <serie>

primary <dirección-ip>

secondary <dirección-ip>

version <valor>

Mandatos de configuración de LDAP (Talk 6)

anonymous-bind [Yes o No]

Especifica si se desea vincular al directorio LDAP de forma anónima o con el nombre y la contraseña de vínculo que ha especificado.

Valor por omisión: Yes

bind-name <nombre>

Solicita la información necesaria para vincularse al servidor LDAP, antes de que pueda realizarse una búsqueda de su directorio. El parámetro *nombre* especifica el nombre distinguido que utiliza el direccionador para identificarse. Si no entra este parámetro, el vínculo se emite como petición anónima.

bind-pw <contr>

Solicita la información necesaria para vincularse al servidor LDAP, antes de que pueda realizarse una búsqueda de su directorio. El parámetro *contr* es la contraseña relacionada con el nombre distinguido. Si no entra este parámetro, el vínculo se emite como petición anónima.

policy-base <serie>

Le solicita entrar una serie de caracteres que se utiliza para definir el ámbito de la búsqueda de políticas en la SRAM del direccionador y el servidor LDAP. Por ejemplo, puede utilizar esta opción para devolver las políticas que sólo se aplican al direccionador A, NHD o IBM-US. La base de política es el nombre distinguido del objeto DeviceProfile en el servidor LDAP.

primary <dirección-ip>

Le solicita la dirección IPv4 del servidor LDAP desde el que se recuperan políticas.

secondary <dirección-ip>

Le solicita la dirección IPv4 de un servidor LDAP de reserva que se utiliza si no se puede alcanzar el servidor por omisión.

version <valor>

Le solicita el número de la versión LDAP soportada por el servidor LDAP.

Valor por omisión: 2 (Los únicos valores aceptables son 2 ó 3).

Set Refresh

Utilice el mandato **set refresh** para habilitar o inhabilitar la renovación automática, una vez al día, de la base de datos de políticas. Si está habilitada, la base de datos de políticas se renueva automáticamente una vez al día a la hora especificada. Esto permite que todos los direccionadores habilitados por la política en la red incorporen automáticamente los cambios de política que se hayan producido en el directorio LDAP. Para restablecer este parámetro, utilice el mandato Talk 5 **reset refresh** de la característica de política.

Sintaxis: set refresh

```
enabled
yes
no
<hora>
```

enabled [yes o no]

Especifica si se realizará la renovación automática.

<hora>

Si ha especificado que sí, designa la hora del día (en un formato de 24 horas) a la que se produce la renovación.

Acceso al indicador de supervisión de política

La parte de la consola de política permite ver políticas que están en la base de datos de política, así como habilitar o inhabilitar políticas individuales. Para acceder al entorno de supervisión de la Política, escriba **talk 5** en el indicador OPCON (*):

```
* t 5
```

A continuación, entre el siguiente mandato en el indicador +:

```
+ feature policy
Policy>
```

Mandatos de supervisión de política

Estos mandatos permiten ver los perfiles definidos en la base de datos de política, así como habilitar o inhabilitar las políticas individuales. La Tabla 46 resume los mandatos de supervisión de política y el resto de esa sección los describe. Entre los mandatos en el indicador `Policy console>`. Puede entrar el mandato y las opciones en una línea, o entrar únicamente el mandato y responder a las solicitudes. Para ver una lista de las opciones de mandato válidas, entre el mandato con un signo de interrogación en lugar de especificar opciones.

Tabla 46. Mandatos de supervisión de política

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado "Cómo obtener ayuda" en la página xxxiv.
Disable	Inhabilita una política que está cargada en la base de datos de política.
Enable	Habilita una política que está cargada en la base de datos de política.
Reset	Renueva o restablece los criterios relativos a la política.
Search	Prueba o depura la actividad entre el cliente y el servidor LDAP.
Status	Visualiza información acerca de la base de datos de política.
List	Visualiza información acerca de la configuración de LDAP y las políticas definidas.
Test	Consulta el motor de política y recupera las reglas que se seleccionaron
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página xxxiv.

Disable

Utilice el mandato **disable** para inhabilitar una política cargada actualmente en la base de datos de políticas. A cualquier paquete de datos que coincida con los criterios de una política que ha inhabilitado, se le aplicarán decisiones por omisión.

Sintaxis: `disable <nombre-política>`

Enable

Utilice el mandato **enable** para habilitar una política cargada actualmente en la base de datos de políticas. En cualquier paquete de datos que coincida con los criterios de una política que ha habilitado, se configurarán decisiones para la política aplicada al mismo.

Sintaxis: `enable <nombre-política>`

Reset

Utilice el mandato **reset** para renovar o restablecer los criterios relacionados con la política.

Sintaxis: `reset ldap-config
policy-database
refresh-time`

ldap-config

Carga dinámicamente en la memoria la configuración de LDAP (tal como se especifica en el mandato **set ldap**). Los cambios se activarán para la siguiente operación de búsqueda. Este mandato también fuerza el restablecimiento de la base de datos de políticas e inactiva el tiempo de renovación de la base de datos de políticas.

policy-database

Renueva la base de datos de política. Detiene todos los túneles, las SA de fase 1 y 2, restablece las estructuras de datos de RSVP y DiffServ, y desecha la base de datos de políticas. A continuación, las políticas se cargan desde el servidor LDAP y se realiza un inicio automático. Mientras se reconstruye la base de datos, no se permitirá ningún paquete de entrada o de salida en el direccionador, salvo los paquetes que entren o salgan del servidor LDAP.

refresh-time

Define la hora a la que la base de datos de políticas se renovará automáticamente con periodicidad diaria. Si ha inhabilitado el tiempo de renovación, la base de datos no se renovará hasta que el direccionador no se vuelva a arrancar o iniciar.

Search

Utilice el mandato **search** para probar o depurar la actividad entre el cliente y el servidor LDAP. Puede realizar búsquedas en el directorio y definir que los resultados se visualicen en talk 5.

Sintaxis: `search filtro
dirección IP`

filtro

Especifica un valor de filtro para la operación de búsqueda.

dirección IP

Especifica la dirección IP del servidor.

Status

Utilice el mandato **status** para visualizar información acerca de la base de datos de políticas.

Sintaxis: `status`

status

Visualiza los resultados de la última renovación de la base de datos de políticas, el tiempo transcurrido y la hora a la que está planificada la próxima.

Ejemplo:

```
Policy>status
Status of Last Search:      Failed
Time since last refresh:   4 seconds
Next Policy Refresh not scheduled
```

List

Utilice el mandato **list** para visualizar información acerca de las configuraciones y las políticas de LDAP.

Sintaxis: `list` `default-policy`
 `ldap`
 `policy`
 `refresh`
 `rule`
 `stats`

default-policy

Lista la política por omisión utilizada durante las renovaciones de base de datos de políticas.

ldap

Lista las configuraciones de LDAP en la SRAM.

policy

basic Lista los componentes de política por su nombre de política lógica. Puede seleccionar una política o listar todas las políticas. La lista muestra los nombres de los componentes de las políticas, tal como se entraron durante la configuración de Talk 6.

complete Igual que `list policy basic`. Muestra además una lista completa de todos los valores de parámetro para cada política lógica.

generated Realiza lo mismo que `list policy basic`, salvo que la lista muestra los nombres de todas las reglas generadas para cada política lógica.

refresh

Lista el estado de renovación de la política (Enable o Disable), así como el tiempo del intervalo de renovación.

rule

Lista información acerca de las reglas generadas, según estas opciones:

basic Lista todas las reglas generadas. Puede seleccionar una regla de la lista, o listar todas las reglas. La lista muestra los nombres de los componentes de las reglas. Los componentes son:

policy name
loaded from (LDAP o local)
state

Mandatos de supervisión de política (Talk 5)

priority

number of hits

profile

validity (seguido de una lista de acciones que consiste en las siguientes) IPSec (and, or)

ISAKMP (and, or)

DiffServ (and, or)

RSVP

complete Realiza lo mismo que rule basic, salvo que la lista muestra los nombres de todos los parámetros para cada componente.

stats

Lista las reglas que se han visto afectadas y el número de actuaciones. Una regla puede tener varias acciones y no todas las acciones se ven afectadas, por lo que esta opción indica también qué acción de la regla se ha visto afectada y cuántas veces.

Test

Utilice el mandato **test** para verificar el funcionamiento de la base de datos de políticas. Permite entrar un conjunto de selectores, que consulta el motor de la política y recupera las reglas coincidentes. Se le solicitan las direcciones de origen y de destino, los puertos de origen y de destino, el ID de protocolo y el valor de TOS. Si coincide una regla, el mandato devuelve su nombre. De lo contrario, indica *No match found (No se ha encontrado ninguna coincidencia)*.

Sintaxis: `test` forwarder
 ISAKMP
 IPSec
 RSVP

forwarder

Simula una consulta de base de datos del motor de reenvío de IP, y devuelve las decisiones de políticas que resultarían de una consulta de ese tipo. El tipo de política devuelta podría incluir información de DiffServ, información de las fases 1 y 2 de IKE y los ID de túnel manual de IPSec.

ISAKMP

Simula una consulta de base de datos de IKE para obtener información sobre la política, y devuelve las decisiones de políticas que resultarían de una consulta de ese tipo. Si utiliza esta opción, debe definir las direcciones de origen y de destino a las direcciones IP de punto final de túnel, y debe definir también el protocolo como 17 y los puertos de origen y destino con el valor 500.

IPSec

Simula una consulta de base de datos de IKE para obtener información sobre la política de fase 2 y devuelve las decisiones de políticas que resultarían de una consulta de ese tipo. Si usa esta opción, debe definir las direcciones de origen y destino a las direcciones IP de punto final de túnel y debe definir también el protocolo como 17 y los puertos de origen y destino con el valor 500.

RSVP

Simula una consulta de base de datos de RSVP y devuelve las decisiones de política de RSVP que resultarían de una consulta de ese tipo.

Utilización de Seguridad de IP

Este capítulo explica cómo utilizar la característica Seguridad de IP; contiene las secciones siguientes:

- “Visión general de la Seguridad de IP”
- “Conceptos de Seguridad de IP” en la página 368
- “Utilización del Intercambio de claves de Internet” en la página 377
- “Utilización de la infraestructura de clave pública” en la página 380
- “Utilización de la seguridad de IP manual (IPv4)” en la página 385
- “Utilización de la seguridad de IP manual” en la página 385

Visión general de la Seguridad de IP

En esta sección se da una visión general de las posibilidades de seguridad de IP para IPv4 y IPv6.

Utilización de túneles seguros

Para proteger los paquetes IP enviados a otro sistema principal, direccionador o cortafuegos, puede configurar un túnel seguro para cada ruta IP que deba ser segura. Un túnel de IPSec es una conexión lógica bidireccional al sistema principal, direccionador o cortafuegos remoto, a través de la cual un direccionador local envía paquetes IP protegidos. Un túnel seguro se identifica con parámetros tales como las direcciones de los sistemas principales de origen y de destino, números de puerto e ID de túnel.

Con IPv4, puede definir un túnel negociado configurando una política de túneles en la base de datos de políticas, o puede crear un túnel manual mediante el mandato Talk 6 **add tunnel**, tal como se muestra en “Configuración del túnel para el direccionador A” en la página 402. Con IPv6, utilice el mandato Talk 6 **add tunnel**.

Para establecer un túnel de IPSec seguro, una política puede especificar la función Cabecera de autenticación (AH) IP (consulte “Cabecera de autenticación IP” en la página 370), que conecta cabeceras de autenticación especiales y la función ESP (Carga de seguridad de encapsulación) (consulte “Carga de seguridad de encapsulación IP” en la página 371), que cifra los datos. La política establece cuál de las siguientes medidas de seguridad se implementan para los paquetes:

- Claves de algoritmo de AH y autenticación de AH (consulte “Configuración de los algoritmos” en la página 392 o “Configuración de los algoritmos” en la página 405, lo que sea más adecuado.)
- Claves de algoritmo de cifrado ESP y de cifrado y descifrado ESP (consulte “Configuración de los algoritmos” en la página 392 o “Configuración de los algoritmos” en la página 405, lo que sea más adecuado.)
- Índices de parámetros de seguridad (SPI) (consulte “Asociaciones de seguridad” en la página 372.)

Nota: Para cada túnel seguro, el remitente y el destinatario deben seleccionar opciones idénticas.

Conceptos de Seguridad de IP

Los paquetes enviados utilizando el Protocolo Internet (IP) pueden convertirse en seguros mediante la característica Seguridad de IP del 2216.

La seguridad, tal como se describe en el documento RFC 2401 - Security Architecture for the Internet Protocol, se compone de las funciones siguientes:

Autenticación

Saber que los datos recibidos son los mismos que los que se enviaron y que el supuesto remitente es el verdadero.

Integridad

Asegurarse de que los datos se transmiten desde el origen al destino sin sufrir alteraciones no detectadas.

Confidencialidad

Comunicarse de tal manera que los destinatarios sepan lo que se ha enviado, pero terceros ajenos a la transferencia no puedan determinar qué es lo que se ha enviado.

Sin desmentido

Comunicarse de tal manera que el destinatario pueda probar que el remitente ha enviado realmente ciertos datos, aunque el remitente pudiese negar posteriormente haberlos enviado.

Nota: En algunos países, no se proporciona soporte de cifrado a causa de las regulaciones de las exportaciones de Estados Unidos; los parámetros de cifrado no se visualizan. No obstante, el algoritmo ESP-NUL está disponible en todos los casos. Para ver una definición del algoritmo ESP-NUL, consulte "Algoritmos de cifrado de ESP" en la página 371.

Terminología de la Seguridad de IP

Los siguientes términos se utilizan al describir temas de IPsec relativos a IPv4:

Cabecera de autenticación (AH)

Área de datos que contiene información de cabecera del paquete, que proporciona la autenticación sobre el origen de los datos, integridad de los datos y protección de la reproducción.

Certificado

Elemento de datos de codificación ASN.1 (según los estándares ITU X.509) que vincula el ID de una entidad final con su clave pública. (En este caso, la entidad final es la entidad de negociación ISAKMP.) La entidad final debe registrar su ID y su clave pública con una autoridad de certificación (CA); para ello, debe someter una petición de certificado. La CA verifica la petición, la firma y la emite hacia la entidad. ISAKMP utiliza el certificado de clave pública durante el proceso de Fase 1 para autenticar los intercambios de mensajes iniciales que configuran la clave secreta maestra (clave criptográfica) entre los direccionadores.

Autoridad de certificación (CA)

Autoridad de confianza que emite certificados digitales X.509 "firmados" que los usuarios de la red deben utilizar para intercambiar datos de usuario seguros mediante ISAKMP. Para participar en intercambios de datos seguros con otras terceras partes habilitadas por ISAKMP, un direccionador debe registrarse con un CA y obtener un certificado digital X.509 que se utilizará en la autenticación.

Signatura digital

Elemento de datos que contiene el ID codificado de un usuario y que pasa a formar parte de un certificado digital X.509. Los usuarios intercambian certificados durante las negociaciones de la Fase 1 para autenticarse entre sí. La signatura se genera realizando una operación de clave pública en un área de datos de entrada que se debe firmar.

Carga de seguridad de encapsulación (ESP)

Función IPsec que puede encapsular y cifrar un datagrama de tal manera que nadie, salvo el destinatario, pueda determinar su contenido. Esto abarca la integridad de los datos y la protección de la reproducción. ESP también proporciona autenticación del origen de los datos. Opera en las modalidades siguientes: de transporte, que sólo cifra la carga del datagrama original, dejando que la información sobre direcciones sea visible para terceros no autorizados, y de túnel, en la que se cifra todo el datagrama original, incluida la cabecera. Así se oculta la información importante sobre las direcciones.

Intercambio de claves de Internet (IKE)

Protocolo derivado de los protocolos ISAKMP y Oakley, que la comunidad de Internet utiliza para intercambiar claves criptográficas y autenticar las partes que se comunican.

ISAKMP

Protocolo de gestión de claves y asociación de seguridad Internet. Esta función configura automáticamente las asociaciones de seguridad y gestiona las claves criptográficas de los paquetes mientras dure un intercambio de datos.

Base de información de gestión (MIB)

Bloque de datos enviado por un direccionador como respuesta a una consulta procedente de una autoridad central y de confianza, que ha solicitado información estadística acerca de las operaciones del direccionador. La autoridad puede detectar problemas en la red y ponerse en contacto con la persona responsable para que emprenda acciones que corrijan esta situación.

Oakley

El protocolo de gestión de claves criptográficas utilizado por ISAKMP.

Secreto perfecto de reenvío (PFS)

Nivel de seguridad de datos obtenido si las negociaciones de la Fase 2 generan nueva información de claves criptográficas para cada negociación. ISAKMP lo consigue habilitando el intercambio de valores Diffie Hellman públicos entre las partes. Esta característica de seguridad impide que un usuario determine una clave criptográfica a partir de una clave comprometida anteriormente.

Negociaciones de la Fase 1

Comunicación entre un remitente y un destinatario que establece una asociación de seguridad ISAKMP y claves criptográficas que protegerán los mensajes ISAKMP que se intercambiarán durante las negociaciones de la Fase 2. La Fase 1 se ejecuta de manera intensiva por el procesador y lo habitual es que se realice de forma infrecuente, tal vez sólo con una periodicidad diaria o semanal.

Negociaciones de la Fase 2

Intercambio de mensajes ISAKMP entre un remitente y un destinatario durante el cual se negocian las asociaciones de seguridad y las claves criptográficas que protegerán los intercambios de datos de los usuarios. Lo habitual es que

Utilización de Seguridad de IP

estas negociaciones se produzcan con frecuencia, tal vez cada dos o tres minutos; se utilizan para renovar las claves criptográficas de forma regular sin que intervenga el usuario.

Proxy

Direccionador que se asigna para que opere en nombre de otro dispositivo de red.

Infraestructura de clave pública (PKI)

Infraestructura utilizada por una CA para vincular el ID del usuario con su clave pública y que distribuye la clave pública vinculada de una manera tal que asegure su seguridad.

Modalidad rápida

Término utilizado para describir las negociaciones de la Fase 2 para asociaciones de seguridad que no sean ISAKMP.

Reproducción

Acto de capturar un datagrama e intentar determinar su contenido, o montar un ataque de denegación de servicio reenviándolo de forma repetida.

Asociación de seguridad (SA)

Área de datos que reúne información acerca de un paquete de datos, tal como su algoritmo criptográfico y su información de clave, las identidades de las partes participantes, etcétera.

Transformar

Colección de información con nombre, acerca de una configuración de las selecciones de autenticación y cifrado.

Cabecera de autenticación IP

La Cabecera de autenticación (AH) se describe en RFC 2402, Cabecera de autenticación IP. Esta cabecera contiene datos de autenticación para el datagrama IP.

Para IPv4 utilizando IPSec negociado, la política asignada a un datagrama implementa una función de autenticación criptográfica que se basa en el protocolo Intercambio de claves de Internet (IKE) y una pareja de claves, pública y privada. Para los túneles manuales de IPv4 y para IPv6, el remitente utiliza una función criptográfica que se basa en una clave de autenticación secreta. En cualquier caso, la función de autenticación criptográfica se aplica al contenido del datagrama. Puede especificar AH de forma aislada o con ESP. Vea "Utilización de AH y ESP" en la página 372 para obtener más detalles.

Algoritmos de autenticación de AH

Un túnel seguro que utiliza una política de túnel de AH debe utilizar uno de los algoritmos de autenticación siguientes:

- Autenticación IP HMAC-MD5 con Prevención de reproducción
- Autenticación IP HMAC-SHA-1 con Prevención de reproducción

Estos algoritmos de AH combinan una función de autenticación de mensaje con clave utilizando hashing criptográfico (código de autenticación de mensaje de hash, cuya abreviatura es HMAC) con una función de prevención de reproducción opcional. La prevención de reproducción utiliza un número de secuencia contenido en la AH para verificar que un paquete no se ha recibido anteriormente. La prevención de reproducción protege al receptor de ataques de denegación de servicio, en los que se envía el mismo paquete de manera repetida y el direccionador está tan

ocupado procesando los paquetes duplicados que no puede procesar el tráfico correcto. Un código de autenticación se aplica a una clave criptográfica secreta y a los datos, y posteriormente a la salida de la clave secreta y a la salida de la primera operación. Vea una ilustración de la forma como se realiza esto para HMAC-MD5 en la Figura 32.

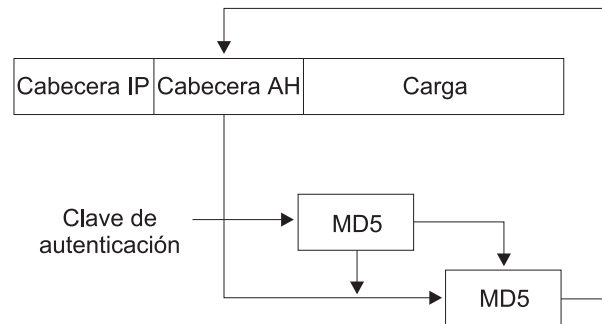


Figura 32. Creación de un mensaje autenticado de HMAC MD5

Carga de seguridad de encapsulación IP

La Carga de seguridad de encapsulación IP (ESP) se describe en el documento RFC 2406 IP Encapsulating Security Payload. ESP cifra una parte del paquete IP o todo para proporcionar confidencialidad, además de la autenticación (opcional) y la integridad. No obstante, si selecciona el algoritmo ESP-NUL, ESP sólo realiza la comprobación de la autenticación y la integridad. Puede especificar ESP de forma aislada o con AH. Vea “Utilización de AH y ESP” en la página 372 para obtener más detalles.

Algoritmos de autenticación de ESP

Los algoritmos disponibles para la autenticación de ESP son los mismos que para AH, que se han indicado anteriormente en la sección “Algoritmos de autenticación de AH” en la página 370.

Algoritmos de cifrado de ESP

Un túnel seguro que utiliza la política de cifrado ESP debe utilizar uno de los algoritmos de cifrado siguientes o el algoritmo ESP-NUL:

- Data Encryption Standard in Cipher Block Chaining Mode (DES-CBC)
- Commercial Data Masking Facility (CDMF)
- Triple DES (3DES)

Nota: Salvo ESP-NUL, los algoritmos de cifrado de ESP están sujetos a las leyes sobre exportaciones de Estados Unidos. Si el 2216 no le permite utilizar algunos de estos algoritmos o ninguno de ellos, es posible que la venta de estos algoritmos esté prohibida en su país. Póngase en contacto con el representante de IBM para obtener más información.

El algoritmo ESP-NUL no cifra los datos cleartext y está disponible en todos los países. Sólo habilita la comprobación de autenticación e integridad de ESP, no el cifrado. Si utiliza ESP-NUL, **debe** utilizar uno de los algoritmos de autenticación de ESP.

Utilización de AH y ESP

Un túnel seguro puede utilizar una de las siguientes selecciones de autenticación/cifrado: AH, ESP, AH-ESP o ESP-AH. Si desea una combinación de AH y ESP, se aplican las siguientes instrucciones:

- La política AH-ESP especifica que, para los paquetes de salida, el cifrado se ejecuta antes que la autenticación. En este caso, la función de autenticación de AH se ejecuta primero en el direccionador de destino, comprobando los paquetes de entrada, y sólo los paquetes que pasen la autenticación se reenviarán a ESP para su descifrado.
- La política ESP-AH especifica que, para los paquetes de salida, la autenticación se ejecuta antes que el cifrado. En este caso, la función ESP descifra primero los paquetes de entrada en el direccionador de destino, y sólo los paquetes que se descifran satisfactoriamente se reenvían a la autenticación de AH.

Asociaciones de seguridad

Una Asociación de seguridad (SA) es una “conexión” simplex que permite dar servicios de seguridad al tráfico transportado por ella. Los servicios de seguridad se permiten para una SA por el uso de AH o ESP, pero no ambas. Si se aplica la protección de AH y ESP a una corriente de datos en tráfico, se crean dos (o más) SA para permitir la protección de dicha corriente. Para asegurar una comunicación bidireccional típica entre dos sistemas principales o entre dos pasarelas de seguridad, se necesitan dos SA (una en cada dirección).

Modalidad de túnel y modalidad de transporte

La modalidad operativa (de túnel o de transporte) determina cómo IPsec gestiona los paquetes IP. La modalidad de túnel es la modalidad por omisión y es necesaria si el direccionador actúa como pasarela de seguridad. Protege los datos en un único segmento de una vía de acceso a través de una red. La modalidad de transporte sólo está permitida cuando el direccionador actúa como sistema principal y protege los datos de extremo a extremo, a lo largo de una vía de acceso completa.

AH y las modalidades operativas

En la modalidad de túnel, la AH se coloca frente al paquete IP y una cabecera IP nueva se crea y se coloca frente a la AH. La cabecera IP del paquete que pasa por el túnel (cabecera interna) transporta las direcciones finales de origen y de destino del paquete. La nueva cabecera IP (cabecera externa) puede contener las direcciones de las pasarelas de seguridad, que son los extremos del túnel. La AH protege todo el paquete nuevo, tanto la nueva cabecera IP como el paquete IP que pasa por el túnel, salvo los campos que pueden variar en la nueva cabecera IP.

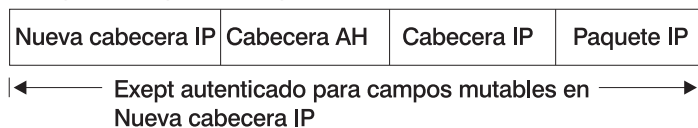
En la modalidad de transporte, la AH se inserta después de la cabecera IP y antes de la cabecera de un protocolo de capa superior, como TCP o UDP. En esta modalidad, AH realiza la autenticación de la cabecera de protocolo de capa superior y el contenido del paquete IP, salvo los campos que pueden variar en la cabecera IP (como la suma de comprobación de período de duración [TTL], indicativo de fragmento, desplazamiento de fragmento y tipo de servicio [TOS]).

La Figura 33 en la página 373 muestra el formato de los datagramas protegidos por AH.

Datagrama original



Datagrama original protegido por modalidad de túnel AH



Datagrama original protegido por modalidad de transporte AH

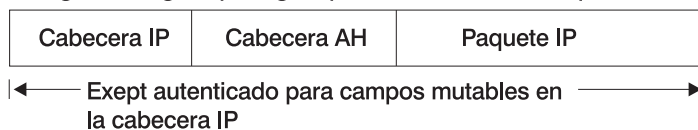


Figura 33. Formato de datagrama protegido por AH

ESP y las modalidades operativas

En la modalidad de túnel, los datos de carga contienen el paquete IP completo y una cabecera IP nueva se crea y se coloca frente a la cabecera ESP. La cabecera IP del paquete que pasa por el túnel (cabecera interna) contiene las direcciones finales de origen y de destino del paquete, mientras que la nueva cabecera IP (cabecera externa) contiene las direcciones de las pasarelas de seguridad. ESP cifra el paquete IP que pasa por el túnel. Si utiliza la autenticación ESP, se realiza la autenticación de la cabecera ESP, el paquete IP que pasa por el túnel y la terminación ESP.

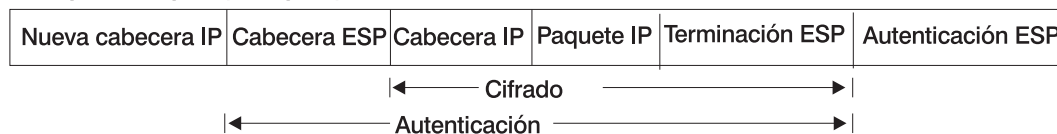
En la modalidad de transporte, los datos de carga contienen datos de protocolo cifrados de capa superior, tales como datos TCP o UDP. Si utiliza la autenticación, se realiza la autenticación de la cabecera ESP, los datos de protocolo de capa superior y la terminación ESP.

La Figura 34 muestra el formato de los datagramas protegidos por ESP.

Datagrama original



Datagrama original protegida por modalidad de túnel ESP



Datagrama original protegido por modalidad de transporte ESP

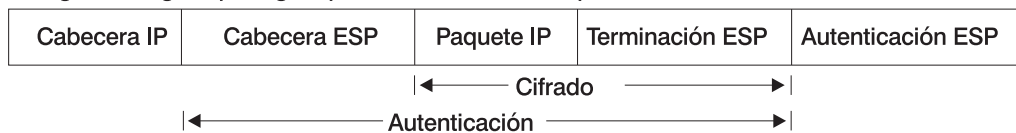
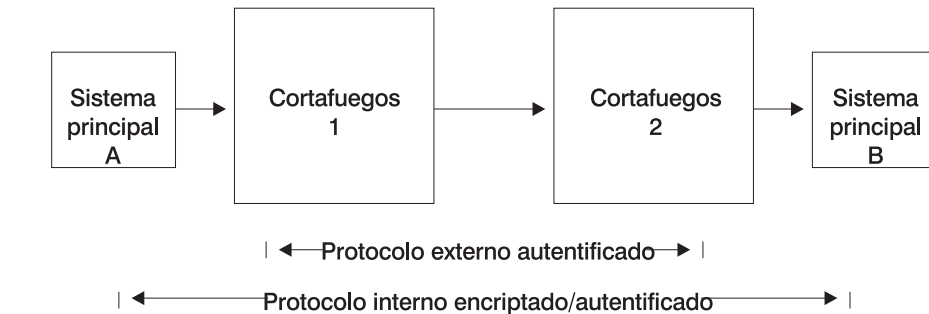


Figura 34. Formato de datagrama protegido por ESP

Anidado de AH y ESP

Puede anidar un protocolo dentro de otra instancia de sí mismo o de otro protocolo. La Figura 35 muestra los efectos de anidar un datagrama protegido por ESP en un túnel de AH.



El sistema principal A utiliza Transporte ESP

Cabecera IP	Cabecera ESP	Paquete IP	Cola ESP	Autent.ESP
-------------	--------------	------------	----------	------------

El cortafuegos 1 utiliza Túnel AH, añadiendo una nueva cabecera IP

Nueva cabecera IP	Cabecera IP	Cabecera ESP	Paquete IP	Cola ESP	Autent.ESP
-------------------	-------------	--------------	------------	----------	------------

El cortafuegos 2 recibe el datagrama en túnel AH, lo autentifica, desprende la cabecera externa y la cabecera AH

Cabecera IP	Cabecera ESP	Paquete IP	Cola ESP	Autent.ESP
-------------	--------------	------------	----------	------------

Figura 35. Anidado de ESP en un túnel de AH

Utilización de la Seguridad de IP con paquetes L2TP

Con IPv4, puede utilizar también IPSec para proteger los paquetes L2TP. Después de crear un túnel L2TP encapsulando una trama L2TP en un paquete UDP, puede encapsular el paquete UDP en un paquete IP cuyas direcciones de origen y de destino definan los extremos del túnel. Entonces puede aplicar los protocolos AH, ESP y ISAKMP al paquete IP. La Figura 36 muestra un paquete L2TP encapsulado por IP, incluyendo PPP y su protocolo de carga para su transmisión a través de Internet.

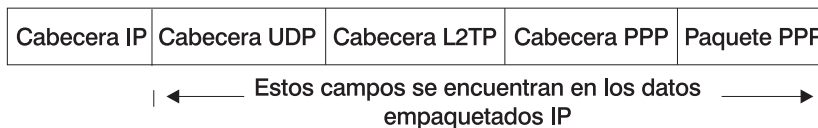


Figura 36. Paquete L2TP protegido por IPSec

Modalidad de túnel en túnel

Para conseguir una mayor seguridad, además de las características de seguridad que ya se han descrito, puede encapsular los paquetes de una corriente de datos en tráfico dos veces, y transmitirlos primero a través de un túnel de IPSec y después a través de otro (túnel en túnel).

Nota: La utilización del cifrado múltiple (utilizando la modalidad de túnel en túnel cuando se realiza el cifrado para ambos túneles) en el direccionador está limitada por las regulaciones sobre exportaciones del Gobierno de Estados Unidos. Sólo está soportado en las cargas de software que están bajo control estricto de exportaciones (cargas de software que dan soporte a RC4 con claves de 128 bits y Triple DES).

Con IPv4, una regla de la base de datos de política designa un paquete para la encapsulación (interna) para el primer túnel y, antes de que se envíe el paquete, la regla hace que el paquete se someta a un segundo túnel para una segunda encapsulación (externa). Con IPv6, una regla del control de acceso de filtro de paquete identifica un paquete para la encapsulación (interna) para el primer túnel y, antes de que se envíe el paquete, una segunda regla hace que el paquete se someta a un segundo túnel para una segunda encapsulación (externa).

Ambos túneles IPSec tienen su origen en el mismo direccionador y sus extremos remotos se encuentran en la misma ubicación física, pero en máquinas distintas. El extremo remoto del primer túnel puede ser una pasarela segura o un sistema principal; el extremo final del segundo túnel *debe* ser un direccionador de pasarela segura. Dado que los túneles tienen destinos diferentes, deben tener direcciones IP remotas distintas. Ambos túneles utilizados para túnel en túnel deben configurarse para la modalidad de túnel, y no se permite un relleno extra en el segundo túnel.

Después de la segunda encapsulación, el paquete se transmite a través del segundo túnel (externo). En el extremo de ese túnel, la encapsulación externa se elimina y el paquete se reenvía al primer túnel (interno), según la información incluida en la cabecera creada por la primera encapsulación de túnel. En el extremo de este túnel, la encapsulación interna se elimina y el paquete se reenvía a su destino final.

Descubrimiento de Unidad de transmisión máxima de vía de acceso

Para IPv4 e IPv6, IPSec da soporte al Descubrimiento de Unidad de transmisión máxima de vía de acceso (PMTU) si el 2216 actúa como pasarela de seguridad. El soporte del Descubrimiento de PMTU es un problema si no se puede fragmentar un paquete. Con IPv4, no se puede fragmentar un paquete si está definido el bit DF (No fragmentar). Con IPv6, los direccionadores intermedios no pueden fragmentar un paquete. En estas situaciones, si el paquete no encaja en un enlace en la vía de acceso desde un extremo al otro del túnel seguro, se envía un mensaje de error ICMP "packet too big" (paquete demasiado grande) al originador del paquete.

Dado que el direccionador actúa como pasarela de seguridad, el paquete de error se devuelve al direccionador de origen en lugar de al originador verdadero del paquete. El direccionador receptor debe pasar la MTU indicada de vuelta al originador verdadero, que puede reducir el tamaño del paquete para que llegue a su destino final. El soporte del Descubrimiento de PMTU se analiza en el documento RFC 2401 - Security Architecture for the Internet Protocol.

Utilización de Seguridad de IP

IPv4 proporciona las opciones siguientes para el valor del bit DF en la cabecera externa del paquete de túnel:

1. Copiar desde la cabecera interna
2. Definir siempre
3. Borrar siempre

Estas opciones están disponibles al configurar la modalidad segura de túnel en túnel; por ejemplo, al utilizar la característica de política **add ipsec-manual-tunn** (IPv4) o el mandato Talk 6 **add tunnel** (IPv6). El bit DF se gestiona de acuerdo a la opción seleccionada, excepto en las condiciones siguientes:

- La MTU del túnel es igual que la MTU mínima.
- El tamaño del paquete de entrada es menor o igual que la MTU mínima.
- El tamaño de paquete encapsulado es mayor que la MTU mínima.

En estas circunstancias, para IPv4, el bit DF no está definido, sea cual sea la configuración, y es posible fragmentar el paquete seguro como sea necesario en la vía de acceso que va al receptor. Para IPv6, el paquete se fragmenta como sea necesario al salir de la pasarela de seguridad, para encajar en la PMTU del túnel. Esta acción especial es necesaria porque el paquete de entrada ya es menor o igual que la MTU mínima, de manera que el sistema principal de origen no reducirá más el tamaño. Si no se permite la fragmentación, este paquete no llegará nunca a su destino final

Dado que los cambios en la topología o la configuración de la red pueden modificar la PMTU, es preciso dejar que el valor de PMTU caduque y restablecerlo a su valor máximo. El valor del temporizador de caducidad es, por omisión, de 10 minutos y se puede configurar con el mandato Talk 6 **set path**. La definición del parámetro de caducidad como 0 inhabilita la caducidad de PMTU.

Diagrama de una red con un túnel de seguridad IP

La Figura 37 en la página 377 muestra un ejemplo de una red con dos túneles IPsec que conectan el direccionador A (con IPsec) con el direccionador B (con IPsec y la Conversión de direcciones de red para IPv4).

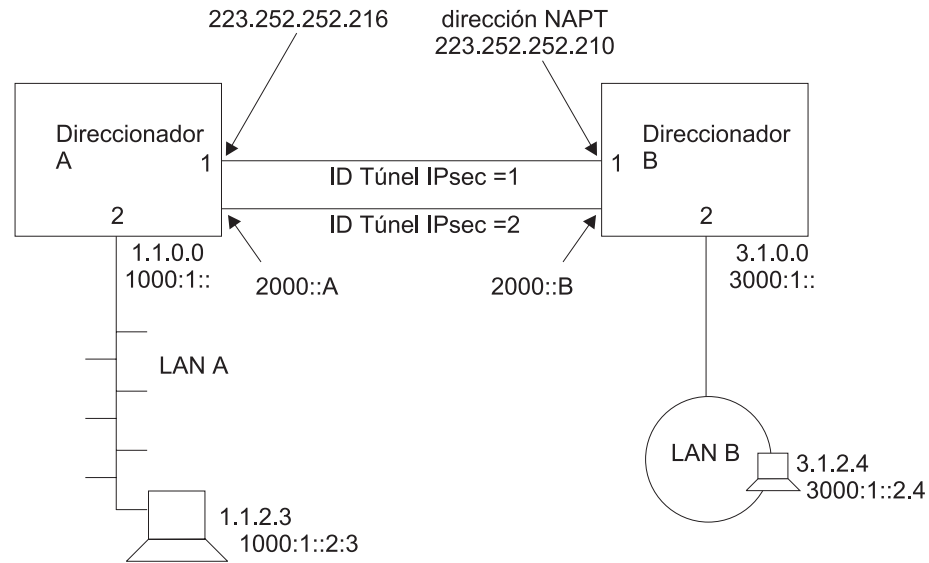


Figura 37. Red con IPsec y NAT

En esta red, un túnel de IPsec con el ID de túnel de IPsec 1 se ha configurado desde la dirección IPv4 223.252.252.216 en el direccionador A a la dirección IPv4 223.252.252.210 en el direccionador B. El direccionador A está configurado para IPsec. El direccionador B está configurado para IPsec y NAT.

Además, en esta red, un túnel de IPsec con el ID de túnel de IPsec 2 se ha configurado desde la dirección IPv6 2000::A en el direccionador A a la dirección IPv6 2000::B en el direccionador B.

Con IPv4, para configurar esta red para IKE, siga los pasos indicados a partir de “Configuración del Intercambio de claves de Internet (IPv4)” en la página 387. Para IPv4 con IPsec manual, siga los pasos indicados a partir de “Configuración de un túnel manual (IPv4)” en la página 402. Para IPv6, siga los pasos indicados a partir de “Configuración de un túnel manual (IPv6)” en la página 406.

Nota: Aunque no tenga previsto utilizar NAT en la red, la descripción de la configuración del direccionador B puede ayudarle a entender con mayor claridad las relaciones entre los parámetros en cada extremo del túnel de IPsec.

Utilización del Intercambio de claves de Internet

En esta sección se explica cómo puede utilizar el Intercambio de claves de Internet (IKE) para automatizar la definición y la creación de asociaciones de seguridad (SA) IPsec. IKE es un estándar soportado por IETF (RFC 2409), que proporciona un procedimiento estándar para que los productos habilitados por IPsec del mismo proveedor o de diferentes proveedores se comuniquen acerca de sus requisitos de seguridad.

IKE proporciona una infraestructura de la que se cumplen los siguientes requisitos de seguridad:

Autenticación de la entidad negociadora remota (entidad similar IKE) Mediante el uso de una clave precompartida o de un certificado digital, IKE realiza la autenticación de la identidad de la entidad con la que se está comunicando, haciendo que demuestre que es lo que afirma ser.

Creación de material de clave idéntico en ambas entidades similares Mediante el mecanismo de clave pública/privada Diffie-Hellman, IKE se encarga del intercambio del componente de clave pública y de la generación independiente de claves idénticas en cada entidad similar.

Proporcionar protección para la negociación de asociaciones de seguridad IPSec Mediante un proceso compuesto de dos fases que se describe en el tema siguiente, IKE se encarga de la creación de asociaciones de seguridad que se utilizan exclusivamente para proteger la negociación de los *túneles* IPSec y para la negociación y creación de *asociaciones de seguridad* que IPSec utiliza para proteger los datos de los usuarios.

Fases del Intercambio de claves de Internet

IKE define dos intercambios de negociación diferenciados: la Fase 1 y la Fase 2. La Fase 1 configura un túnel seguro entre las dos entidades similares IKE, que proporcionará protección para las negociaciones posteriores de túnel de IPSec. Se producen las acciones siguientes durante la Fase 1, en el orden indicado:

1. Las entidades similares IKE negocian y acuerdan las características de la asociación de seguridad de la Fase 1. Estas características incluyen el algoritmo de cifrado que se utilizará para cifrar *las comunicaciones IKE*, el algoritmo hash que se debe utilizar, el método de autenticación y el grupo Diffie-Hellman que deberá utilizarse al generar las claves.
2. Se generan las claves Diffie-Hellman y las partes públicas se intercambian con la entidad similar IKE. Estas claves se utilizan para generar claves de cifrado que cifrarán las negociaciones de la Fase 1 y, además, permitirán la generación de claves que utilizarán los túneles IPSec.
3. Se realiza la autenticación de la entidad similar IKE mediante uno de los dos métodos soportados: la modalidad de clave precompartida y la modalidad de firma.

En la modalidad de clave precompartida, ambas entidades similares IKE, mediante un proceso previo fuera de línea, han intercambiado una clave que se utiliza durante la Fase 1 para realizar la autenticación de la entidad similar. Configure la clave precompartida mediante el mandato **add user** de la característica de política.

En la modalidad de firma, se utiliza un certificado digital X.509 firmado para proporcionar las claves que se utilizarán para cifrar y descifrar las cargas de los mensajes de la Fase 1. Una firma y verificación satisfactorias incluye la autenticación de la entidad similar. Para ver un análisis detallado de la modalidad de firma y el uso de los certificados digitales, consulte "Utilización de la infraestructura de clave pública" en la página 380.

Las negociaciones de la Fase 1 pueden efectuarse utilizando una de estas dos modalidades de intercambio:

- La modalidad principal utiliza seis mensajes para ejecutar las negociaciones de la Fase 1 y cifra las identidades de las entidades similares negociadoras.
- La modalidad agresiva utiliza tres mensajes para realizar las negociaciones de la Fase 1. En los dos primeros mensajes, las entidades similares intercambian identidades no protegidas.

Negociación de un túnel de seguridad de IP

El proceso analizado en este tema se produce cuando un direccionador se prepara para enviar un paquete cuyos atributos coinciden con los definidos en una regla incluida en una base de datos de política. La negociación de un túnel se realiza en dos fases. Durante la Fase 1, el direccionador remitente inicia la comunicación transmitiendo el primer mensaje de un intercambio de seis, que establece las opciones de seguridad que se utilizarán durante la Fase 2. El receptor responde y ambas partes negocian las características de la asociación de seguridad (SA) ISAKM, los algoritmos de autenticación y cifrado que se deberán utilizar, y realizan la autenticación mutua de sus identidades. Durante la Fase 2, las partes intercambian tres mensajes en total, para negociar las SA y las claves que se deberán utilizar para proteger los datagramas IP que se envíen mutuamente. La Fase 1 se desarrolla de la manera siguiente:

1. Mensaje 1: el remitente propone cómo se realizará la actividad de comunicación: el método de autenticación (por ejemplo, firmas digitales), el algoritmo de autenticación (por ejemplo, HMAC-MD5) y el algoritmo de cifrado (por ejemplo, DES-CBC) que se utilizarán.
2. Mensaje 2: el receptor indica al remitente a cuál de las opciones de seguridad dará soporte, en el caso de que haya alguna.
3. Mensaje 3: el remitente transmite su valor público Diffie Hellman y un valor aleatorio a partir del cual se crearán las claves de cifrado.
4. Mensaje 4: el receptor transmite su propio valor público Diffie Hellman y un valor aleatorio a partir del cual se crearán las claves de cifrado. En este momento, ambas partes crean las claves públicas y privadas y la información relativa a las claves que se deberán utilizar en los intercambios de mensajes ISAKMP.
5. Mensaje 5: el remitente transmite una firma digital y puede incluir un certificado digital X.509 firmado por una autoridad de certificación (CA) de confianza. Si el remitente no incluye un certificado válido, el receptor debe utilizar el protocolo LDAP para obtener un certificado de una CA de confianza, un servidor DNS seguro y una antememoria local segura que correlacione los certificados utilizados anteriormente con sus respectivos valores de ID, o bien puede solicitar un certificado del remitente, que debe enviarlo de inmediato.
6. Mensaje 6: después de verificar la firma digital del remitente, el receptor transmite al remitente la misma clase de información de identificación acerca de sí mismo.

En este momento, ambas partes han realizado mutuamente la autenticación, han acordado las características de la SA y han derivado claves e información relativa a las claves para la gestión de las SA ISAKMP. Ahora, las partes entran en la Fase 2 para negociar las SA y las claves que no son ISAKMP, que se utilizarán para proteger los datagramas IP intercambiados entre ellas. La Fase 2 continúa de la manera siguiente:

1. Mensaje 1: el remitente propone una SA ISAKMP transmitiendo una selección de los algoritmos AH o ESP e incluye también otra información relativa a la seguridad.
2. Mensaje 2: el receptor indica al remitente qué propuesta ha seleccionado e incluye información relativa a la seguridad.
3. Mensaje 3: el remitente transmite un registro hash de varios elementos para indicar al receptor que está listo para continuar utilizando los protocolos de

seguridad negociados. Cuando el receptor verifica la información, el enlace está completo y las partes pueden empezar a intercambiar corrientes de datos protegidas.

Utilización de la infraestructura de clave pública

En esta sección se explica cómo utilizar la infraestructura de clave pública (PKI). Mediante PKI, IKE da soporte a la modalidad de signatura de clave pública para realizar la autenticación de entidades IKE. Aunque este release da soporte a la modalidad de clave precompartida, que no requiere el soporte PKI, esta modalidad contiene una desventaja inherente. Para realizar la autenticación, requiere que configure cada entidad IKE con la clave precompartida de cada una de sus entidades similares. Esto limita gravemente la escalabilidad de las operaciones de IKE. Las modalidades de signatura basada en clave pública o de cifrado público proporcionan mucha mejor escalabilidad. En este release, se utiliza el certificado digital X.509 en las negociaciones de Fase 1 de la modalidad de signatura para realizar la autenticación de las entidades IKE.

Asigne una identidad a cada entidad IKE que desee que participe en las negociaciones de IKE, especificando un valor exclusivo en el campo del ID de ISAKMP al configurar su perfil de política de usuario. Cada entidad de IKE realiza la autenticación de su identidad con sus entidades similares.

Se está definiendo y desarrollando PKI para dar soporte a la operación de clave pública. En PKI, un certificado digital X.509 vincula la clave pública de una entidad con su supuesta identidad. Una entidad IKE puede extraer la clave pública contenida en un certificado. A continuación, puede realizar una operación de clave pública para realizar la autenticación de la identidad de una entidad similar que participe en una negociación IKE. Se utiliza una clave pública para la modalidad de signatura de IKE. En esta modalidad, el firmante utiliza su clave privada para firmar la signatura digital. El receptor extrae la clave pública del firmante del certificado y la utiliza para verificar la signatura. La función de certificado digital proporciona una manera escalable de que la entidad IKE realice la autenticación de otra entidad IKE.

Configuración de PKI

En este release se supone que ambas entidades IKE en una negociación utilizan la misma CA. Antes de iniciar las negociaciones de IKE utilizando la signatura, debe configurar PKI para el direccionador. También debe generar la clave privada del direccionador y el certificado del direccionador, y debe haber bajado el certificado de la CA raíz. Los pasos siguientes explican cómo configurar PKI:

1. Genere el par de claves y solicite el certificado.

Dado que la operación de clave pública implica un par de claves (la modalidad de signatura utiliza la clave privada para la signatura y la clave pública para la verificación), debe generar un par de claves para el direccionador. Para una petición de certificado, debe enviar la clave pública generada a la CA para que se ponga en un certificado digital X.509. Después, cada entidad similar IKE potencial podrá extraer esta clave pública del certificado emitido por la CA. La clave privada reside en el direccionador, se mantiene en secreto y sólo es conocida para el direccionador.

En esta versión, puede emitir un mandato **certificate request**, que realiza lo siguiente:

- a. Genera un par de claves, cuya longitud de clave puede especificar como de 512, 768 ó 1024 bits. La clave privada generada permanece en la antememoria.
 - b. Solicita que entre información para incluirla en la petición de certificado (por ejemplo, el ID de direccionador en forma de dirección IP, nombre de dominio o nombre de correo electrónico).
 - c. Crea una petición de certificado (en formato PKCS#10) que contiene la clave pública generada y la información que ha entrado.
 - d. Realiza un TFTP de la petición de certificado a un sistema principal.
2. Emite el certificado (fuera del direccionador)

La CA recibe la petición de certificado PKCS#10. La CA puede verificar manualmente la petición y emitir un certificado. El certificado contiene la clave pública del direccionador y la información que ha entrado. La CA firma el certificado utilizando su clave privada, convirtiéndolo así en información digital de confianza mientras para el usuario sea de confianza la CA firmante. El certificado ya está listo para su utilización en las negociaciones de IKE. (Este proceso se encuentra fuera del ámbito de la operación del direccionador y no se analiza con más detalles en este manual.)

3. Baje el certificado del direccionador

Una vez que la CA haya emitido el certificado, PKI podrá bajarlo al direccionador. Según cómo la CA publique el certificado, PKI podrá utilizar TFTP o LDAP para bajarlo.

Tenga en cuenta que la clave privada y la pública en el certificado del direccionador deben coincidir para realizar una operación de clave pública como una signatura digital. Cuando PKI baje el certificado al direccionador, la clave privada generada con la clave pública deberá estar en la antememoria de clave del direccionador. El certificado bajado es inútil si pierde la clave privada correspondiente. Esto quiere decir que, desde el momento que se emita la petición de certificado, hasta que se baje el certificado, el usuario **no debe** volver a iniciar o a cargar el direccionador, borrar la antememoria ni emitir una nueva petición de certificado. Cualquiera de estas operaciones destruirá la clave privada en el direccionador que ejecuta la antememoria.

4. Baje el certificado de la CA

Para verificar el certificado de la entidad similar IKE, PKI debe obtener el certificado de la CA raíz de la entidad similar. Este release da soporte a la operación de CA de nivel único, lo que significa que es preciso asignar las entidades IKE a la misma CA. Cada entidad IKE (en este caso, cada direccionador) debe bajar el certificado de la CA (mediante TFTP o LDAP) para verificar que es válido el certificado recibido de la entidad similar.

5. Guarde y vuelva a cargar el certificado

Después de que el direccionador haya obtenido el certificado, la clave privada coincidente y el certificado de la CA, puede iniciar la negociación de IKE. Dado que lo habitual es que un certificado sea válido durante varios meses o años, tal vez desee guardar el certificado y la clave privada en la SRAM, de tal manera que no tendrá que emitir una petición de certificado y bajarlo cada vez que vuelva a cargar o a iniciar el direccionador. Esta versión proporciona los mandatos **cert save** y **cert load** para guardar o recuperar el certificado y la clave privada en la SRAM.

Utilización de Seguridad de IP

Tenga en cuenta que el certificado y la clave privada del direccionador se deben procesar como un par (por ejemplo, siempre se guardan o se recuperan juntos de la SRAM).

Utilice los mandatos de Talk 6 para configurar y listar la información de servidor de TFTP y LDAP, tal como se muestra en los ejemplos siguientes:

Ejemplo: Add Server (T6)

```
Config>f ipsec
IP Security feature user configuration
IPsec config>pki
PKI config>add server
Name ? (max 65 chars) []? test
Enter server IP Address []? 8.8.8.8
Transport type (Choices: TFTP/LDAP) [TFTP]?
PKI config>
```

Ejemplo: List Server Configuration (T6)

```
PKI config>li server
```

- 1) Name: SERVER1
Type: TFTP
IP addr: 8.8.8.8

- 2) Name: TEST
Type: TFTP
IP addr: 8.8.8.8

Ejemplo: List Root Certificate (T6)

PKI config>li cert

Root CA certificate:

SRAM Name: R1
 Subject Name: /c=US/o=ibm/ou=nhd
 Issuer Name: /c=US/o=ibm/ou=nhd
 Validity: 1998/12/19 -- 2018/12/19

Default Root Cert: No

SRAM Name: R2
 Subject Name: /c=US/o=ibm/ou=nhd
 Issuer Name: /c=US/o=ibm/ou=nhd
 Validity: 1998/12/19 -- 2018/12/19

Default Root Cert: Yes

Router Certificate:

SRAM Name: B1
 Subject Name: /c=CA/o=Entrust Technologies/ou=PartnerCA/cn=ibm3
 Issuer Name: /c=CA/o=Entrust Technologies/ou=PartnerCA
 Subject alt Name: 1.1.1.1
 Key Usage: Sign & Encipherment
 Validity: 1998/10/29 -- 2001/10/29

Default Cert: No

SRAM Name: B2
 Subject Name: /c=CA/o=Entrust Technologies/ou=PartnerCA/cn=ibm3
 Issuer Name: /c=CA/o=Entrust Technologies/ou=PartnerCA
 Subject alt Name: 1.1.1.1
 Key Usage: Sign & Encipherment
 Validity: 1998/10/29 -- 2001/10/29

Default Cert: Yes

SRAM Name: B3
 Subject Name: /c=CA/o=Entrust Technologies/ou=PartnerCA/cn=ibm3
 Issuer Name: /c=CA/o=Entrust Technologies/ou=PartnerCA
 Subject alt Name: 1.1.1.1
 Key Usage: Sign & Encipherment
 Validity: 1998/10/29 -- 2001/10/29

Default Cert: No

SRAM Name: YYY
 Subject Name: /c=CA/o=Entrust Technologies/ou=PartnerCA/cn=ibm3
 Issuer Name: /c=CA/o=Entrust Technologies/ou=PartnerCA
 Subject alt Name: 1.1.1.1
 Key Usage: Sign & Encipherment
 Validity: 1998/10/29 -- 2001/10/29

Default Cert: No

Ejemplo: Certificate Request (T5)

```
PKI Console>cert-req
Enter the following part for the subject name
Country Name(Max 16 characters) []? us
Organization Name(Max 32 characters) []? IBM
Organization Unit Name(Max 32 characters) []? NHD
Common Name(Max 32 characters) []? router1
Key modulus size
[512]?
Certificate subject-alt-name type:
1--IPv4 Address
2--User FQDN
3--FQDN
Select choice [1]?
Enter an IPv4 addr) []? 12.1.1.1
Generating a key pair. This may take some time. Please wait ...
PKCS10 message successfully generated
Enter tftp server IP Address []? 8.8.8.8
Remote file name (max 63 chars) [/tmp/tftp_pkcs10_file]?
Memory transfer starting.
.Memory transfer completed - successfully.
Certificate request TFTP to remote host successfully.
Private Key Alias [ROUTER_KEY]? local
Generated private key LOCAL stored into cache
```

Ejemplo: List Router Certificate (T5)

```
PKI Console>li cert
Router certificate
Serial Number: 909343811
Subject Name: /c=CA/o=Entrust Technologies/ou=PartnerCA/cn=ibm3
Issuer Name: /c=CA/o=Entrust Technologies/ou=PartnerCA
Subject alt Name: 1.1.1.1
Key Usage: Sign & Encipherment
Validity: 1998/10/29 -- 2001/10/29

Root CA certificate
Serial Number: 914034740
Subject Name: /c=US/o=ibm/ou=nhd
Issuer Name: /c=US/o=ibm/ou=nhd
Validity: 1998/12/19 -- 2018/12/19
```

Ejemplo: Cert Save (T5)

```
PKI Console>cert-save
Enter type of certificate to be stored into SRAM:
1)Root certificate;
2)Box certificate with private key;
Select the certificate type (1-2) [2]?
SRAM Name for certificate and private key []? yyy
Load as default router certificate at initialization?? [No]:
Private key YYY written into SRAM
Both Certificate and private key saved into SRAM successfully
PKI Console>
```

Ejemplo: Cert Load (T5)

```
PKI Console>cert-load
Enter type of certificate to be stored into SRAM:
  1)Root certificate;
  2)Box certificate with private key;
Select the certificate type (1-2) [2]?
Name []? yyy
Box certificate and private key saved into cache successfully
PKI Console>
```

Utilización de la seguridad de IP manual (IPv4)

La característica de seguridad de IP contenida en IPv4 para el 2216, junto con la característica de política y otros procesos relacionados con IPSec, proporciona autenticación, integridad, confidencialidad y sin desmentido. Para implementar IPSec manualmente, debe preconfigurar una política que contenga un subconjunto de opciones de IPSec en una base de datos de política para definir el perfil y el período de validez del túnel manual. También puede preconfigurar el conjunto completo de opciones de IPSec (política) en la base de datos, de manera que, cuando un direccionador habilitado por la política, se prepare para enviar un paquete IPSec, negociará y establecerá dinámicamente las opciones de IPSec con el direccionador de destino, según el contenido de la política. Para definir un túnel manual, consulte “Configuración de la Seguridad de IP manual (IPv4)” en la página 392. Para obtener una explicación de las opciones de política, consulte “Utilización de la característica de política” en la página 307.

Utilización de la seguridad de IP manual

La característica de seguridad de IP contenida en IPv6 para el 2216 proporciona autenticación, integridad y confidencialidad. Para definir un túnel manual, consulte “Configuración de la Seguridad de IP manual (IPv6)” en la página 404.

Configuración y supervisión de la Seguridad de IP

Este capítulo describe cómo configurar y supervisar la seguridad de IP y cómo utilizar los mandatos de supervisión de la seguridad de IP. Para IPv4, las secciones “Utilización de la característica de política” en la página 307 y “Configuración y supervisión de la característica de política” en la página 343 proporcionan información adicional acerca de la configuración y supervisión de las políticas de seguridad de IP. Este capítulo contiene las secciones siguientes:

- “Configuración del Intercambio de claves de Internet (IPv4)”
- “Configuración de la Infraestructura de clave pública (IPv4)” en la página 388
- “Obtención de un certificado” en la página 388
- “Mandatos de configuración de la Infraestructura de clave pública” en la página 389
- “Configuración de la Seguridad de IP manual (IPv4)” en la página 392
- “Acceso al entorno de configuración de la Seguridad de IP” en la página 393
- “Mandatos de la configuración manual de la Seguridad de IP” en la página 393
- “Configuración de un túnel manual (IPv4)” en la página 402
- “Configuración de la Seguridad de IP manual (IPv6)” en la página 404
- “Acceso al entorno de configuración de la Seguridad de IP” en la página 405
- “Mandatos de la configuración manual de la Seguridad de IP” en la página 406
- “Configuración de un túnel manual (IPv6)” en la página 406
- “Supervisión de la Seguridad de IP manual (IPv4)” en la página 410
- “Supervisión de la Seguridad de IP manual (IPv6)” en la página 423

Nota: Si crea un túnel de IPSec para transportar tráfico TN3270, APPN-ISR o APPN-HPR, y piensa dar prioridad a este tráfico mediante BRS, tendrá que utilizar la característica de valor de bit de precedencia de IPv4 de BRS. Consulte “Utilización del proceso de bits de precedencia de IP Versión 4 para el tráfico SNA en túneles seguros IP y fragmentos secundarios” en la página 10 para obtener más información.

Configuración del Intercambio de claves de Internet (IPv4)

Este tema explica cómo configurar el Intercambio de claves de Internet (IKE).

Antes de establecer un túnel de IPSec, debe:

1. Configurar los atributos de paquetes que utilizarán el túnel y las acciones resultantes que deben emprenderse (política).
2. Configurar las opciones de cifrado y autenticación que desee.

Para obtener detalles acerca de cómo llevar a cabo estas tareas, consulte las secciones “Utilización de la característica de política” en la página 307, “Configuración y supervisión de la característica de política” en la página 343 y “Configuración de la Infraestructura de clave pública (IPv4)” en la página 388.

Configuración de la Infraestructura de clave pública (IPv4)

Este tema explica cómo configurar la Infraestructura de clave pública (PKI) con IPv4.

Antes de establecer un túnel de IPSec, debe:

1. Crear un par de clave criptográfica pública/privada y obtener un certificado digital de una Autoridad de certificación (CA) de confianza. Consulte “Obtención de un certificado” para obtener detalles.
2. Decidir cuáles son los algoritmos de IPSec, las SA y otras opciones que desea utilizar para los direccionadores cuyas políticas está configurando. Consulte “Negociación de un túnel de seguridad de IP” en la página 379 y los temas posteriores para obtener detalles.
3. Configurar IKE y la base de datos de política. Consulte “Configuración del Intercambio de claves de Internet (IPv4)” en la página 387, “Utilización de la característica de política” en la página 307 y “Configuración y supervisión de la característica de política” en la página 343 para obtener detalles.

Obtención de un certificado

Antes de establecer un túnel de IPSec, se debe seleccionar y registrar con una Autoridad de certificación (CA), tal como se describe en “Utilización de la infraestructura de clave pública” en la página 380. La CA devuelve un certificado digital X.509 firmado, que le permite identificarse y establecer su propia autenticación ante otras partes existentes en la red. El certificado consiste en un ID digital codificado (signatura) y un par de claves criptográficas pública/privada. Realice lo siguiente:

1. Identifique una CA y obtenga su dirección de servidor.
2. Configure las opciones de recuperación del depósito de certificados, utilizando el mandato PKI Talk 6 **add ldapserver** o **add tftpserver**, tal como se describe en “Mandatos de configuración de la Infraestructura de clave pública” en la página 389.
3. Cree un par de claves pública/privada mediante el mandato PKI Talk 5 **certificate request**, tal como se describe en “Mandatos de supervisión de la Infraestructura de clave pública” en la página 413. Puede hacer esto en el direccionador o de forma remota, por ejemplo, actuando como administrador de la Red privada virtual (VPN), en cuyo caso deberá cifrar y transferir el par de claves al direccionador de forma segura.
4. Someta una petición de certificado inicial a la CA mediante el mandato PKI Talk 5 **certificate request**, tal como se describe en “Mandatos de supervisión de la Infraestructura de clave pública” en la página 413. La petición se envía en un mensaje PKCS#10 a través de correo electrónico o FTP. La CA vincula el par de claves con el certificado, lo firma con la clave privada de la CA y lo guarda en un depósito central (LDAP o FTP) o lo devuelve al usuario en un mensaje PKCS#7. Normalmente, la validez de un certificado dura varios meses o más y después se renueva. Esto identifica qué miembros de una red siguen siendo de confianza.
5. Guarde el certificado en la SRAM de un direccionador mediante el mandato PKI Talk 5 **certificate save**, tal como se describe en “Mandatos de supervisión de la Infraestructura de clave pública” en la página 413.

Notas:

1. Para visualizar una lista de los registros de certificado que hay en la SRAM, utilice el mandato PKI Talk 6 **list certificate**, tal como se describe en “Mandatos de configuración de la Infraestructura de clave pública” en la página 389.
2. Para suprimir los registros de certificado de la SRAM, utilice el mandato PKI Talk 6 **delete certificate** tal como se describe en “Mandatos de configuración de la Infraestructura de clave pública” en la página 389.
3. Para eliminar la necesidad de volver a someter una petición de certificado durante unas negociaciones de IPsec en el futuro, utilice el mandato PKI Talk 5 **certificate load** tal como se describe en “Mandatos de supervisión de la Infraestructura de clave pública” en la página 413 para cargar el certificado recibido en la antememoria.

Mandatos de configuración de la Infraestructura de clave pública

Add

Utilice el mandato PKI Talk 6 **add** para configurar el servidor del depósito de certificados y su ubicación.

Sintaxis:

add server

server Especifica que la operación de adición se refiere a un servidor.

Ejemplo 1: adición de un servidor

```
PKI config>add server
Name ? (max 65 chars) []? myldap
Enter server IP Address []? 8.8.8.9
Transport type (Choices: TFTP/LDAP) [TFTP]? ldap
LDAP search timeout value [3]?
LDAP retry interval (mins) [1]?
LDAP server port number [389]?
LDAP version [2]?
Bind to the server anonymously? [No]:
Enter your bind DN: []? c=us o=ibm
Enter your bind PW: []? testldap
```

Change

Utilice el mandato PKI Talk 6 **change** para modificar el servidor del depósito de certificados y su ubicación.

Sintaxis:

change

server

server Especifica que la operación de adición se refiere a un servidor.

Ejemplo 1: modificación de un servidor

Mandatos de configuración de la Infraestructura de clave pública

```
PKI config>change server
Name []? myldap
Enter server IP Address []? 8.8.8.7
Server type will continue to be LDAP
LDAP search timeout value [3]?
LDAP retry interval (mins) [1]?
LDAP server port number [389]?
LDAP version [2]?
Enter your bind DN: [c=us o=ibm]?
Enter your bind PW: [testldap]?
```

Delete

Utilice el mandato PKI Talk 6 **delete** para suprimir un registro de certificado o un registro de clave privada de la SRAM de un direccionador, o bien para suprimir un servidor.

Sintaxis:

delete

- certificate
- private-key
- server

certificate

Especifica que la operación de supresión se refiere a uno o más registros de certificado.

all Especifica que se deben suprimir todos los registros de certificado.

id Especifica el ID del registro de certificado que debe suprimirse.

Ejemplo 1: supresión de un certificado

```
PKI config>delete certificate
Cert Name []? test
Enter the type of the certificate:
Choices: 1-Root CA Cert, 2-Router Cert
Enter (1-2): [2]?
Box Certificate [TEST] deleted successfully
Corresponding private Key [TEST] deleted successfully
```

Ejemplo 2: supresión de claves privadas

```
PKI config>delete private-keys
Private Key Name []? test
Private Key [TEST] deleted successfully
Corresponding box certificate [TEST] deleted successfully
```

Ejemplo 3: supresión de registros del servidor

```
PKI config>delete server
Name []? myldap
Server MYLDAP deleted successfully
```

private-key

Especifica que la operación de supresión se refiere a uno o más registros de clave privada.

server Especifica que la operación de supresión se refiere a un servidor.

List

Utilice el mandato PKI Talk 6 **list** para listar los registros de certificado o de clave en la SRAM de un direccionador.

Sintaxis:

```
list certificates  
private-keys  
servers
```

certificates

Especifica que la operación de listar se refiere a los registros de certificados.

private-keys

Especifica que la operación de listar se refiere a los registros de clave privada.

servers Especifica que la operación de listar se refiere a los registros de servidor.

Ejemplo 1: listar certificados

```
PKI config>list certificates
```

```
Root CA certificate:  
SRAM Name: B  
Subject Name: /c=US/o=ibm/ou=nhd  
Issuer Name: /c=US/o=ibm/ou=nhd  
Validity: 1998/12/19 2:2:21 -- 2018/12/19 2:32:21  
Default Root Cert: Yes
```

```
Router Certificate:  
SRAM Name: W  
Subject Name: /c=US/o=ibm/ou=nhd/cn=testip  
Issuer Name: /c=US/o=ibm/ou=nhd  
Subject alt Name: 1.1.1.1  
Key Usage: Sign & Encipherment  
Validity: 1999/1/19 23:24:27 -- 2002/1/19 23:54:27  
Default Cert: No
```

Ejemplo 2: listar claves privadas

```
PKI config>list private-keys  
Private Keys In SRAM:
```

```
1) Name W
```

Configuración de la Seguridad de IP manual (IPv4)

Ejemplo 3: listar registros de servidor

```
PKI config>list servers
1) Name: SERVER1
   Type: LDAP
   IP addr: 1.1.1.2
     LDAP search timeout (secs): 10
     LDAP retry interval (mins): 3
     LDAP server port number: 390
     LDAP version: 2
     Anonymous bind ?: y

2) Name: TEST
   Type: TFTP
   IP addr: 8.8.8.8
```

Configuración de la Seguridad de IP manual (IPv4)

Esta sección describe las opciones de configuración disponibles para IPsec manual con IPv4. Todas las funciones de IPsec se aplican a IPv4.

Realice los pasos siguientes para configurar un túnel manual de IPsec:

1. Cree el túnel de IPsec.
2. Restablezca IPsec.
3. Configure la política para el túnel manual (perfil, validez y política).
4. Restablezca la política.

Configuración de los algoritmos

Puede configurar políticas de túnel con los algoritmos que aparecen en la Tabla 47.

Política de túnel	Algoritmos
AH, AH-ESP o ESP-AH	<ul style="list-style-type: none">• Algoritmo de autenticación de AH local: obligatorio• Algoritmo de autenticación AH remoto: opcional
ESP, AH-ESP o ESP-AH	<ul style="list-style-type: none">• Algoritmo de cifrado local: obligatorio• Algoritmo de cifrado remoto: opcional• Algoritmo de autenticación ESP local: opcional• Algoritmo de autenticación ESP remoto: opcional <p>Nota: Si la carga de software no incluye el cifrado, no verá los parámetros relativos al cifrado.</p>

Una política de túnel utiliza un algoritmo local en los paquetes de salida y un algoritmo remoto en los paquetes de entrada. El algoritmo local para el direccionador en el extremo más próximo de un túnel debe coincidir con el algoritmo remoto para el direccionador en el extremo más alejado del túnel. Los valores de los algoritmos remotos son opcionales y toman por omisión el valor de los algoritmos locales

correspondientes. El algoritmo de autenticación ESP local es opcional porque la autenticación ESP también lo es.

Configuración de claves de cifrado

Para cada algoritmo local que configure, debe configurar también una clave que sea idéntica a la clave para el algoritmo correspondiente en el sistema principal remoto. Vea la descripción de las claves para el mandato **add tunnel** en “Mandatos de la configuración manual de la Seguridad de IP”.

Acceso al entorno de configuración de la Seguridad de IP

Para acceder al entorno de configuración de la Seguridad de IP, entre **t 6** en el indicador OPCON (*) y, a continuación, entre la siguiente secuencia de mandatos en el indicador Config>:

```
Config> feature ipsec
IP Security feature user configuration
IPsec config>ipv4
IPV4-IPsec config>
```

Mandatos de la configuración manual de la Seguridad de IP

Esta sección describe los mandatos de configuración de la Seguridad de IP. Entre estos mandatos en el indicador IPV4-IPsec config>.

Tabla 48. Resumen de los mandatos de configuración de la Seguridad de IP

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxiv.
Add tunnel	Añade un túnel seguro.
Change tunnel	Cambia los valores de los parámetros de la configuración de túnel seguro.
Delete tunnel	Suprime un túnel seguro.
Disable	Inhabilita todo el proceso de Seguridad de IP de manera segura (los paquetes que coinciden con los filtros de paquete se eliminan), inhabilita todo el proceso de Seguridad de IP de manera no segura (los paquetes que coinciden con los filtros de paquete pasan), o inhabilita un túnel seguro.
Enable	Habilita todo el proceso de Seguridad de IP, o habilita un túnel seguro.
List	Lista información acerca de la información global de la Seguridad de IP, o información acerca de los túneles definidos.
Set	Define diversas opciones de IPSec.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiv.

Add Tunnel

Utilice el mandato **add tunnel** para añadir los parámetros para definir un túnel de IPSec.

Sintaxis:

add tunnel...

tunnel-name

Parámetro opcional para etiquetar el túnel. Debe ser un valor exclusivo en el 2216.

Valores válidos: 15 caracteres como máximo; el primer carácter debe ser una letra; no pueden utilizarse espacios en blanco.

Valor por omisión: ninguno

lifetime

Tiempo, en minutos, que el túnel puede estar activo. El valor 0 indica que la existencia del túnel no caduca nunca.

Valores válidos: 0 - 525600 (0 = sin caducidad; 525600 = 365 días)

Valor por omisión: 46080 (32 días)

encapsulation-mode

La manera en que está encapsulado el paquete IP. En la modalidad de túnel, se encapsula todo el paquete IP completo y se crea una cabecera IP nueva; en la modalidad de transporte, la cabecera IP no se encapsula. Si un extremo del túnel seguro es un direccionador, **debe** utilizarse la modalidad de túnel, según el borrador de arquitectura de seguridad del IETF (Internet Engineering Task Force).

Valores válidos: túnel (*TUNN*) o convertir (*TRANS*)

Valor por omisión: túnel (*TUNN*)

tunnel-policy

Una de las cuatro opciones que definen la política de túnel: Cabecera de autenticación IP (AH), Carga de seguridad de encapsulación (ESP) o combinaciones de estos protocolos (AH-ESP y ESP-AH). En AH-ESP, el cifrado ESP se ejecuta en primer lugar en los paquetes de salida; en ESP-AH, la autenticación de AH se ejecuta en primer lugar en los paquetes de salida. Algunos parámetros son exclusivos de ESP o de AH. Los parámetros de cifrado sólo se configuran si se selecciona ESP, AH-ESP o ESP-AH; los parámetros de autenticación sólo se configuran si se selecciona AH, AH-ESP o ESP con la autenticación.

Valores válidos: AH, ESP, AH-ESP, ESP-AH

Valor por omisión: AH-ESP

local-IP-address

Dirección IP para este extremo del túnel.

Valores válidos: una dirección IP válida que se ha configurado para una interfaz o como dirección interna del 2216.

Valor por omisión: una de las direcciones IP configuradas para el direccionador

local-spi

Una asociación de seguridad es una conexión de seguridad unidireccional que utiliza AH o ESP para proteger el tráfico de la conexión. El índice de parámetros de seguridad (SPI) es un valor arbitrario de 32 bits que identifica de manera exclusiva una de las dos asociaciones de seguridad (de entrada o de salida) asociadas a este túnel seguro. Este parámetro, que es obligatorio, identifica el SPI esperado en este túnel para los paquetes de entrada recibidos en el extremo local del túnel. Este valor no puede emparejar el SPI local de otro túnel con la misma dirección IP local. Sea cual sea la política de túnel (ESP, AH, AH-ESP o ESP-AH), sólo se configura un SPI local para el tráfico de entrada para un túnel IP seguro.

Valores válidos: cualquier valor de 32 bits que sea mayor que 255

Valor por omisión: 256

local-encryption-algorithm

El algoritmo de cifrado utilizado para ESP en los paquetes de salida enviados desde el direccionador local, que es obligatorio al configurar ESP. En algunos países, es posible que algunos de estos algoritmos, o todos ellos, no estén disponibles debido a las normas sobre exportaciones de Estados Unidos. Este algoritmo de cifrado debe coincidir con el algoritmo de cifrado remoto.

El algoritmo ESP-NULl evita que ESP realice el cifrado. Este algoritmo está disponible en todos los países. Si se selecciona ESP-NULl, es preciso activar ESP para la autenticación, seleccionando uno de los algoritmos de autenticación HMAC-MD5 o HMAC-SHA-1.

Valores válidos: DES-CBC, CDMF, 3DES o ESP-NULl

Valor por omisión: DES-CBC

local-encryption-key

Clave o claves utilizada(s) con el algoritmo de cifrado ESP local. Deben coincidir con las claves correspondientes que están configuradas en el extremo opuesto del túnel seguro. Esta clave no se configura cuando se selecciona el algoritmo de cifrado ESP-NULl.

Valores válidos:

- Para DES-CBC: 16 caracteres hexadecimales (0 - 9, a - f, A - F)
- Para CDMF: 16 caracteres hexadecimales (0 - 9, a - f, A - F)
- Para 3DES: tres claves distintas, ninguna de las cuales es la misma, cada una de ellas de 16 caracteres hexadecimales (0 - 9, a - f, A - F)

Valor por omisión: ninguno

padding-for-local-encryption

Tamaño en bytes del relleno adicional que se añade a los paquetes ESP de salida. El relleno adicional puede utilizarse para ocultar el tamaño de los paquetes IP que se cifran, cuando el algoritmo de cifrado da como resultado un paquete cifrado con el mismo tamaño que el paquete original. Los valores de relleno de ESP deben ser múltiplos de 8. Si se configura un valor que no es divisible por 8, este valor se redondea al valor siguiente que sea divisible por 8.

Cuando el algoritmo de cifrado es ESP-NULl, el relleno no es necesario, porque añade un byte al tamaño original del paquete. Si el relleno está configurado para el cifrado local, el valor se pasará por alto.

Valores válidos: 0 - 120

Valor por omisión: 0

local-ESP-authentication

Selecciona, si se desea, la autenticación ESP local. La autenticación es necesaria si el algoritmo de cifrado es ESP-NULL.

Valores válidos: Yes o No

Valor por omisión: Yes

local-authentication-algorithm

Algoritmo de autenticación utilizado en los paquetes de salida. Es un parámetro opcional para ESP y no es obligatorio a menos que se seleccione la autenticación ESP. Para AH, AH-ESP o ESP-AH, este parámetro es obligatorio. El algoritmo de autenticación utilizado debe coincidir con el algoritmo de autenticación remoto utilizado en el otro extremo del túnel de IPsec.

Valores válidos: HMAC-MD5 o HMAC-SHA

Valor por omisión: HMAC-MD5

local-authentication-key

Clave utilizada con el algoritmo de autenticación local. Debe coincidir con la clave equivalente que está configurada en el extremo opuesto del túnel de IPsec. Es obligatoria si la política es AH, AH-ESP o ESP-AH, o si la política es ESP y se ha configurado el algoritmo de autenticación ESP local.

Valores válidos:

- para HMAC-MD5: 32 caracteres hexadecimales (0 - 9, a - f, A - F)
- para HMAC-SHA: 40 caracteres hexadecimales (0 - 9, a - f, A - F)

Valor por omisión: ninguno

remote-IP-address

Dirección IP correspondiente al extremo remoto del túnel. Es un parámetro obligatorio.

Valores válidos: una dirección IP válida

Valor por omisión: ninguno

remote-spi

Una asociación de seguridad es una conexión de seguridad unidireccional que utiliza AH o ESP para proteger el tráfico de la conexión. El índice de parámetros de seguridad (SPI) es un valor arbitrario de 32 bits que identifica de manera exclusiva una de las dos asociaciones de seguridad (de entrada o de salida) asociadas a este túnel seguro. Este parámetro, que es obligatorio, identifica el SPI esperado en ESP o AH para los paquetes de entrada destinados al sistema principal remoto. Este valor no puede emparejar el SPI remoto de otro túnel con la misma dirección IP remota. Sea cual sea la política de túnel (ESP, AH, AH-ESP o ESP-AH), sólo se configura un SPI local para el tráfico de salida para un túnel de IPsec seguro.

Valores válidos: cualquier valor de 32 bits que sea mayor que 255

Valor por omisión: 256

remote-encryption-algorithm

Algoritmo de descifrado que se utiliza en los paquetes de entrada recibidos del sistema principal remoto. Debe coincidir con el algoritmo de cifrado local.

El algoritmo ESP-NULl evita que ESP realice el cifrado. Si se selecciona ESP-NULl, es preciso activar ESP para la autenticación, seleccionando uno de los algoritmos de autenticación HMAC-MD5 o HMAC-SHA-1.

Valores válidos: DES-CBC, CDMF, 3DES o ESP-NULl

Valor por omisión: valor del algoritmo de cifrado local

remote-encryption-key

Clave o claves utilizada(s) con el algoritmo de cifrado ESP remoto. Deben coincidir con las claves correspondientes que están configuradas en el extremo opuesto del túnel seguro. Esta clave no se configura cuando se selecciona el algoritmo de cifrado ESP-NULl.

Valores válidos:

- Para DES-CBC: 16 caracteres hexadecimales (0 - 9, a - f, A - F)
- Para CDMF: 16 caracteres hexadecimales (0 - 9, a - f, A - F)
- Para 3DES: tres claves distintas, ninguna de las cuales es la misma, cada una de ellas de 16 caracteres hexadecimales (0 - 9, a - f, A - F)

Valor por omisión: ninguno

verification-of-remote-encryption-padding

Determina si debe verificarse el tamaño del relleno de cifrado en los paquetes recibidos.

Valores válidos: Yes o No

Valor por omisión: No

padding-for-remote-encryption

Tamaño en bytes del relleno adicional que se espera en los paquetes ESP recibidos. Este parámetro es obligatorio y sólo es válido si el valor de *verification-of-remote-encryption-padding* es Yes. Los valores de relleno de ESP deben ser múltiplos de 8. Si se configura un valor que no sea divisible por 8, este valor se redondea al valor siguiente que sea divisible por 0.

Valores válidos: 0 - 120

Valor por omisión: 0

remote-ESP-authentication

Selecciona, si se desea, la autenticación de ESP remota para los paquetes de entrada.

Valores válidos: Yes o No

Valor por omisión: Yes

remote-authentication-algorithm

Algoritmo de autenticación utilizado para los paquetes de entrada. Es un parámetro opcional para ESP y no es obligatorio a menos que se seleccione la autenticación ESP. Para AH o combinaciones de AH y ESP (AH-ESP o ESP-AH), este parámetro es obligatorio. El algoritmo de autenticación utilizado debe coincidir con el algoritmo de autenticación local utilizado en el extremo alejado del túnel de IPsec.

Valores válidos: HMAC-MD5 o HMAC-SHA

Valor por omisión: HMAC-MD5

remote-authentication-key

Clave utilizada con el algoritmo de autenticación remoto. Debe coincidir con la clave equivalente que está configurada en el extremo opuesto del túnel seguro. Es obligatoria en AH, AH-ESP y ESP-AH, y también en ESP si se ha configurado el algoritmo de autenticación de ESP remoto.

Valores válidos:

- para HMAC-MD5: 32 caracteres hexadecimales (0 - 9, a - f, A - F)
- para HMAC-SHA: 40 caracteres hexadecimales (0 - 9, a - f, A - F)

Valor por omisión: ninguno

enable-replay-prevention

Especifica si está habilitada la prevención de reproducción. Si está habilitada, se supervisan los números de secuencia de las cabeceras de seguridad de IP para prevenir que el receptor del túnel procese paquetes duplicados. No se recomienda el uso de la prevención de reproducción, ya que es preciso desactivar la asociación de seguridad del túnel cuando el contador de números de secuencia de un remitente alcanza su límite. Cuando sucede esto, se necesita una intervención manual para reiniciar la asociación de seguridad existente o crear una nueva.

Además, si la prevención de reproducción está habilitada y restablece IPSec mediante el mandato **reset ipsec**, debe asegurarse de que también se restablece IPSec en el direccionador del otro extremo del túnel de IPSec. Esto es necesario para volver a inicializar el número de secuencia en ambos extremos del túnel. Si se restablece IPSec en un extremo del túnel, pero no en el otro, es posible que los direccionadores de cada extremo del túnel eliminen paquetes debido a una discrepancia en los números de secuencia.

Valores válidos: Yes o No

Valor por omisión: No

DF-bit

Especifica la gestión del bit No fragmentar (DF) en la cabecera externa para los túneles seguros de la modalidad de túnel. Este bit puede definirse en las cabeceras de IPv4 para especificar que no se puede fragmentar el paquete. El parámetro DF-bit indica al 2216 cómo debe gestionar el bit DF en los paquetes de entrada: si debe copiar en la cabecera externa el valor del bit DF encontrado en la cabecera interna, o si debe definir o borrar el bit en la cabecera externa.

Si el bit DF está definido y el paquete no puede fragmentarse, IPSec utilizará la función Descubrimiento de MTU de vía de acceso (PMTU). Consulte “Descubrimiento de Unidad de transmisión máxima de vía de acceso” en la página 375 para obtener más información.

Valores válidos: Copy, Set, Clear

Valor por omisión: Copy

enable-tunnel

Especifica si este túnel está habilitado. El túnel habilitado no filtrará paquetes hasta que se haya configurado un filtro de paquetes para definir la interfaz a través de la cual operará este túnel de IPSec, e IP se haya restablecido o reiniciado en el 2216. Puede utilizar el mandato **reset ip** para restablecer IP.

Valores válidos: Yes o No

Valor por omisión: Yes

Change Tunnel

Utilice el mandato **change tunnel** para modificar un parámetro de túnel de IPsec. IPsec configurado anteriormente por el mandato **add tunnel**.

Sintaxis:

change tunnel...

Consulte el mandato **add tunnel** para ver una lista de los parámetros que pueden modificarse.

Delete Tunnel

Utilice el mandato Talk 6 **delete tunnel** para suprimir un túnel de IPsec.

Sintaxis:

delete tunnel

tunnel-id

tunnel-name

all

tunnel-id Especifica el identificador del túnel de IPsec que se va a suprimir.

Valores válidos: 1 - 65535

Valor por omisión: 1

tunnel-name

Especifica el nombre del túnel de IPsec que se va a suprimir.

Valores válidos: cualquier nombre de túnel configurado

Valor por omisión: ninguno

all

Especifica que se van a suprimir todos los túneles de IPsec que hay en esta interfaz.

Disable

Utilice el mandato **disable** para inhabilitar el túnel de IPsec, o para inhabilitar todos los túneles de IPsec de manera segura (los paquetes que coinciden con los filtros de IPsec se eliminan) o insegura (los paquetes que coinciden con los filtros de IPsec pasan).

Sintaxis:

disable

ipsec drop

ipsec pass

tunnel ...

ipsec drop

Inhabilita la seguridad de IP en el direccionador de manera segura. Se inhabilitarán todos los túneles de IPsec, pero se utilizará la información de túneles seguros en las reglas de filtros de paquetes para identificar los paquetes que coincidan con los filtros de paquetes de túnel de IPsec. Los paquetes coincidentes se eliminarán.

Mandatos de la configuración manual de la Seguridad de IP

ipsec pass

Inhabilita la seguridad de IP en el direccionador de manera no segura. Se inhabilitarán todos los túneles de IPSec. Los paquetes que coincidan con los filtros de paquetes de túnel de IPSec se reenviarán como tráfico ordinario.

tunnel *tunnel-id tunnel-name* all

Inhabilita la seguridad de IP en un túnel específico o en todos los túneles.

tunnel-id

Especifica el identificador del túnel seguro que se va a inhabilitar.

Valores válidos: 1 - 65535

Valor por omisión: 1

tunnel-name

Especifica el nombre del túnel seguro que se va a inhabilitar.

Valores válidos: cualquier nombre de túnel configurado

Valor por omisión: ninguno

all Todos los túneles.

Enable

Utilice el mandato **enable** para habilitar el protocolo de Seguridad de IP en todas las interfaces o en un único túnel. Debe habilitar IPSec en el direccionador de manera global antes de que se activen los túneles de IPSec habilitados individualmente.

Sintaxis:

enable

ipsec
tunnel ...

ipsec

Habilita la seguridad de IP a través del direccionador.

tunnel *tunnel-id tunnel-name* all

Habilita la seguridad de IP en un túnel específico o en todos los túneles.

tunnel-id

Especifica el identificador del túnel seguro que se va a habilitar.

Valores válidos: 1 - 65535

Valor por omisión: 1

tunnel-name

Especifica el nombre del túnel seguro que se va a habilitar.

Valores válidos: cualquier nombre de túnel configurado

Valor por omisión: ninguno

all Todos los túneles.

List

Utilice el mandato **list** para visualizar la configuración actual de la Seguridad de IP. Los túneles globales incluyen todos los túneles del direccionador, tanto los activos como los definidos. Todos los túneles incluye todos los configurados en esta interfaz, tanto los activos como los definidos. Los túneles activos son los que están activos actualmente; los túneles definidos están definidos, pero no activos. Para IPv4, también se listan los certificados seleccionados en la SRAM de un direccionador.

Sintaxis:

list ...

all

status

tunnel

active id-túnel nombre-túnel all

defined id-túnel nombre-túnel all

Ejemplo 1: lista de todos los túneles de IPsec

```
IPsec config>list all
```

```
IPsec is ENABLED
```

```
IPsec Path MTU Aging Timer is 20 minutes
```

```
Defined Manual Tunnels:
```

ID	Name	Local IP Addr	Remote IP Addr	Mode	State
1	test	1.1.1.1	2.1.1.1	TUNN	Enabled
2	test2	1.1.1.1	1.1.1.3	TRANS	Enabled

```
Tunnel Cache:
```

ID	Local IP Addr	Remote IP Addr	Mode	Policy	Tunnel Expiration
2	1.1.1.1	1.1.1.3	TRANS	ESP	*****
1	1.1.1.1	2.1.1.1	TUNN	AH	*****

Configuración de un túnel manual (IPv4)

Ejemplo 2: lista de un túnel de IPsec con la política ESP y el algoritmo ESP-NULL

```
IPsec config>li tun 1000
```

Tunnel ID	Name	Mode	Policy	Life	Replay Prev	Rcv Win	IPsec Vers	State
1000	t1000	TUNN	ESP	46080	No	---	V2	Enabled

```
Handling of DF bit in outer header: COPY
```

```
Local Information:
```

```
IP Address: 10.11.12.10
Authentication: SPI: ----- Algorithm: -----
Encryption: SPI: 1234 Encryption Algorithm: NULL
Extra Pad: 0
ESP Authentication Algorithm: HMAC-MD5
```

```
Remote Information:
```

```
IP Address: 10.11.12.11
Authentication: SPI: ----- Algorithm: -----
Encryption: SPI: 1234 Encryption Algorithm: NULL
Verify Pad?: No
ESP Authentication Algorithm: HMAC-MD5
```

Set

Utilice el mandato **set** para controlar el valor de PMTU del túnel.

Sintaxis:

```
set path-mtu-age-timer
```

path-mtu-age-timer

Especifica el tiempo (en minutos) que transcurrirá hasta que el 2216 restaure el valor de PMTU del túnel a su valor máximo.

Valor por omisión: 10 (0 significa que está inhabilitado)

Configuración de un túnel manual (IPv4)

Este tema proporciona información acerca de la configuración de un túnel de IPv4 manual para la red que se muestra en la Figura 37 en la página 377.

Configuración del túnel para el direccionador A

El siguiente ejemplo muestra cómo configurar un túnel manual de IPsec para el direccionador A en la red que se muestra en la Figura 37 en la página 377 utilizando IPv4.

```

Config> feature ipsec
IP Security feature user configuration
IPsec config>ipv4
IPv4-IPsec config>add tunnel
Adding tunnel 1
Tunnel Name (optional)? tunnelone
Tunnel Lifetime, in minutes (0-525600) [46080]?
Tunnel Encapsulation Mode (TUNN or TRANS) [TUNN]?
Tunnel Policy (AH, ESP, AH-ESP, ESP-AH) [AH-ESP]? AH
Local IP Address [1.1.1.1]? 223.252.252.216
Local Authentication SPI (256-65535) [256]?
Local Authentication Algorithm (HMAC-MD5, HMAC-SHA) [HMAC-MD5]?
Local Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Local Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Remote IP Address [0.0.0.0]? 223.252.252.210
Remote Authentication SPI (1-65535) [256]?
Remote Authentication Algorithm (HMAC-MD5, HMAC-SHA) [HMAC-MD5]?
Remote Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Remote Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Enable replay prevention? [No]:
Copy, set, or clear DF bit in outer header (COPY,SET,CLEAR) [COPY]?
Do you wish to enable this tunnel? [Yes]:
IPv4-IPsec config>

```

Como puede ver en este ejemplo, se le solicitarán los parámetros que tiene que proporcionar. La configuración de un túnel seguro de ESP, AH-ESP o ESP-AH necesita unos parámetros similares.

Nota: Los valores de las claves no se visualizan cuando se entran. Por consiguiente, no son visibles en este ejemplo. Si las claves de la autenticación HMAC-MD5 fueran visibles, vería 32 caracteres hexadecimales. Por ejemplo, una clave podría tener el siguiente valor:
X'1234567890ABCDEF1234567890ABCDEF'.

Configuración del túnel para el direccionador B

En el direccionador B, debe configurar el mismo túnel manual de IPsec que se configuró para el direccionador A, el túnel de IPsec 1. La dirección IP local de este túnel en el direccionador B es 223.252.252.210 y la dirección IP remota es 223.252.252.216. Todos los demás parámetros de túnel de IPsec deben coincidir con los parámetros que se configuraron para el direccionador A.

Ejemplo: configuración manual de un túnel de Seguridad de IP con ESP

Tenga en cuenta que se le solicitará que defina el bit DF cuando el túnel esté en la modalidad de túnel y la política de túnel sea ESP. Este ejemplo sólo muestra la configuración del túnel de IPsec, no la de los filtros de paquetes.

Configuración de la Seguridad de IP manual (IPv6)

```
IPV4-IPsec config>add tunnel
Adding tunnel 2
Tunnel Name (optional)? tunneltwo
Tunnel Lifetime, in minutes (0-525600) [46080]?
Tunnel Encapsulation Mode (TUNN or TRANS) [TUNN]?
Tunnel Policy (AH,ESP,AH-ESP,ESP-AH) [AH-ESP]? ESP
Local IP Address [1.1.1.1]?
Local Encryption SPI (256-65535) [256]?
Local Encryption Algorithm (DES-CBC,CDMF,3DES, NULL) [DES-CBC]?
Do you wish to change the Local Encryption Key? [No]:
Additional Padding for Local Encryption (0-120) [0]?
Do you wish to use local ESP authentication? [Yes]:
Remote IP Address [0.0.0.0]?
Remote Encryption SPI (1-65535) [256]?
Remote Encryption Algorithm (DES-CBC,CDMF) [DES-CBC]?
Do you wish to change the Remote Encryption Key? [No]:
Do you wish to perform verification of remote encryption padding? [No]:
Do you wish to use remote ESP authentication? [No]:
Copy, set or clear DF bit in outer header (COPY,SET,CLEAR) [COPY]?
Do you wish to enable this tunnel? [Yes]:
IPV4-IPsec config>
```

Ejemplo: configuración manual de un túnel de seguridad de IP con ESP y ESP-NULL

Tenga en cuenta que la autenticación es obligatoria.

```
IPV4-IPsec config>add tunnel
Adding tunnel 3
Tunnel Name (optional)? tunne13
Tunnel Lifetime, in minutes (0-525600) [46080]?
Tunnel Encapsulation Mode (TUNN or TRANS) [TUNN]?
Tunnel Policy (AH,ESP,AH-ESP,ESP-AH) [AH-ESP]? ESP
Local IP Address [1.1.1.1]?
Local Encryption SPI (256-65535) [256]? 1234
Local Encryption Algorithm (DES-CBC,CDMF,3DES,NULL) [DES-CBC]? null
Additional Padding for Local Encryption (0-120) [0]?
Local ESP Authentication Algorithm (HMAC-MD5,HMAC-SHA) [HMAC-MD5]?
Local ESP Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Local ESP Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Remote IP Address [0.0.0.0]? 10.11.12.11
Remote Encryption SPI (1-65535) [1234]?
Remote Encryption Algorithm (DES-CBC,CDMF,3DES,NULL) [NULL]?
Do you wish to perform verification of remote encryption padding? [No]:
Remote ESP Authentication Algorithm (HMAC-MD5,HMAC-SHA) [HMAC-MD5]?
Remote ESP Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Remote ESP Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Enable replay prevention? [No]:
Copy, set or clear DF bit in outer header (COPY,SET,CLEAR) [COPY]?
Do you wish to enable this tunnel? [Yes]:
IPV4-IPsec config>
```

Configuración de la Seguridad de IP manual (IPv6)

Esta sección describe las opciones de configuración disponibles para IPSec manual con IPv6. Todas las funciones de IPSec se aplican a IPv6. Observe los siguientes cambios en las preguntas de configuración de IPSec cuando configure IPSec para IPv6:

- Debe entrar las direcciones en el formato de direcciones de IPv6 (por ejemplo, 8:0:9:8::1).
- No se le solicitará el valor del bit DF.

Realice los pasos siguientes para configurar un túnel manual de IPSec:

1. Cree el túnel de IPSec.
2. Restablezca IPSec.
3. Configure las reglas de filtro.
4. Restablezca IPV6.

Configuración de los algoritmos

Puede configurar políticas de túnel con los algoritmos que aparecen en la Tabla 49.

Política de túnel	Algoritmos
AH, AH-ESP o ESP-AH	<ul style="list-style-type: none"> • Algoritmo de autenticación AH local: obligatorio • Algoritmo de autenticación AH remoto: opcional
ESP, AH-ESP o ESP-AH	<ul style="list-style-type: none"> • Algoritmo de cifrado local: obligatorio • Algoritmo de cifrado remoto: opcional • Algoritmo de autenticación ESP local: opcional • Algoritmo de autenticación ESP remoto: opcional <p>Nota: Si la carga de software no incluye el cifrado, no verá los parámetros relativos al cifrado.</p>

Una política de túnel utiliza un algoritmo local en los paquetes de salida y un algoritmo remoto en los paquetes de entrada. El algoritmo local para el direccionador en el extremo más próximo de un túnel debe coincidir con el algoritmo remoto para el direccionador en el extremo más alejado del túnel. Los valores de los algoritmos remotos son opcionales y toman por omisión el valor de los algoritmos locales correspondientes. El algoritmo de autenticación ESP local es opcional porque la autenticación ESP también lo es.

Configuración de claves de cifrado

Para cada algoritmo que configure, debe configurar también una clave que sea idéntica a la clave para el algoritmo correspondiente en el sistema principal remoto. Vea la descripción de las claves para el mandato **add tunnel** en “Mandatos de la configuración manual de la Seguridad de IP” en la página 393.

Acceso al entorno de configuración de la Seguridad de IP

Para acceder al entorno de configuración de la Seguridad de IP, entre **t 6** en el indicador OPCON (*) y, a continuación, entre la siguiente secuencia de mandatos en el indicador Config>:

Configuración de un túnel manual (IPv6)

```
Config> feature ipsec
IP Security feature user configuration
IPsec config>ipv6
IPV6-IPsec config>
```

Mandatos de la configuración manual de la Seguridad de IP

Consulte “Mandatos de la configuración manual de la Seguridad de IP” en la página 393 para ver una descripción de los mandatos de configuración de la Seguridad de IP que están disponibles para IPv6. Los mandatos de IPv6 son los mismos que los utilizados para IPv4, a menos que se indique lo contrario. Entre los mandatos en el indicador IPV6-IPsec config>.

Configuración de un túnel manual (IPv6)

Consulte la red de ejemplo que aparece en la Figura 37 en la página 377 mientras lee este tema. El túnel de IPsec 1 tiene un extremo en la interfaz 1 del direccionador A. El direccionador A se configurará para IPsec. Realice los pasos siguientes para configurar manualmente un túnel de IPsec:

1. Cree el túnel de IPsec.
2. Cree un filtro de paquete de salida en la interfaz del direccionador que es el extremo del túnel de IPsec.
3. Cree reglas de control de acceso para los filtros de paquetes.
4. Restablezca IPsec.
5. Restablezca IPv6.

Creación del túnel de Seguridad de IP para el direccionador A

El siguiente ejemplo muestra cómo crear el túnel de IPsec 1 para el direccionador A.

```
Config> feature ipsec
IP Security feature user configuration
IPsec config> ipv6
IPV6-IPsec config> add tunnel
IPsec Tunnel ID (1 - 65535) [1]
Tunnel Name (optional)? tunnelone
Tunnel Lifetime, in minutes (0-525600) [46080]?
Tunnel Encapsulation Mode (TUNN or TRANS) [TUNN]?
Tunnel Policy (AH, ESP, AH-ESP, ESP-AH) [AH-ESP]? AH
Local IP Address [1000:1::1]? 2000::A
Local Authentication SPI (256-65535) [256]?
Local Authentication Algorithm (HMAC-MD5, HMAC-SHA) [HMAC-MD5]?
Local Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Local Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Remote IP Address [0::0]? 2000::B
Remote Authentication SPI (1-65535) [256]?
Remote Authentication Algorithm (HMAC-MD5, HMAC-SHA) [HMAC-MD5]?
Remote Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Remote Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Enable replay prevention? [No]:
Do you wish to enable this tunnel? [Yes]:
IPV6-IPsec config>
```

Como puede ver en este ejemplo, se le solicitarán los parámetros que tiene que proporcionar. La configuración de un túnel seguro de ESP, AH-ESP o ESP-AH necesita unos parámetros similares.

Nota: Los valores de las claves no se visualizan cuando se entran. Por consiguiente, no son visibles en este ejemplo. Si las claves de la autenticación HMAC-MD5 fueran visibles, vería 32 caracteres hexadecimales. Por ejemplo, una clave podría tener un valor como el siguiente:
X'1234567890ABCDEF1234567890ABCDEF'.

Configuración de filtros de paquetes para el direccionador A

Después de haber creado el túnel de IPSec para el direccionador A, debe configurar un filtro de paquetes IP. La creación del filtro de paquetes *out-router-A* se muestra en el ejemplo siguiente. Consulte las secciones IPv6 Filtering y Access Control del capítulo Using IPv6 del manual *Consulta de configuración y supervisión de protocolos Volumen 1* para obtener más información acerca de la configuración de filtros de paquetes y reglas de control de acceso de IPv6.

```
*talk 6
Config> Protocol IPv6
Internet protocol user configuration
IPv6 Config> set access-control on
IPv6 Config> add packet-filter
Packet-filter name [ ]? out-router-A
Filter incoming or outgoing traffic? [IN]? OUT
Which interface is this filter for [0]? 1
IPv6 Config> update packet-filter
Packet-filter name [ ]? out-router-A
Packet-filter 'out-router-A' Config>
```

Configuración de las reglas de control de acceso de filtros de paquetes para el direccionador A

El paso siguiente consiste en configurar las reglas de control de acceso de filtros de paquetes. Cree dos reglas de control de acceso en el filtro de paquetes de salida *out-router-A*.

Las reglas de control de acceso en el filtro de paquetes de salida realizarán las siguientes funciones:

- Una regla de control de acceso define el rango de las direcciones de origen y de destino de los paquetes que se van a pasar al túnel de IPSec.
- La otra regla de control de acceso permite que el tráfico de IPSec pase a través del filtro de paquetes.

Configure la primera regla de control de acceso para el filtro de paquetes *out-router-A*. Esta regla de control de acceso pasa los paquetes desde la red 1000:1:: a la red de destino 3000:1:: que está conectada al direccionador B.

```
IPv6 Config> update packet-filter
Packet-filter name [ ]? out-router-A
Packet-filter 'out-router-A' Config> add access
Enter type [E]? IS
Internet source [0::0]? 1000:1::
Prefix Length [64]? 64
Internet destination [0::0]? 3000:1::
Prefix Length [64]? 64
Enter IPsec Tunnel ID [1]? 2
Packet-filter 'out-router-A' Config>
```

La segunda regla de control de acceso de *out-router-A* permite que los paquetes seguros pasen entre ambos extremos del túnel de IPSec.

Configuración de un túnel manual (IPv6)

```
Packet-filter 'out-router-A' Config> add access
Enter type [E]? I
Internet source [0::0]? 2000::A
Prefix Length [64]? 64
Internet destination [0::0]? 2000::B
Prefix Length [64]? 64
Packet-filter 'out-router-A' Config>
```

Como sucede con los demás filtros de paquetes, tal vez quiera configurar una regla comodín de control de acceso para *out-router-A*, que permita el paso del tráfico que no coincida con las reglas de control de acceso.

Restablecimiento de la Seguridad de IP y de IP en el direccionador A

Después de acabar de configurar la política, utilice el mandato Talk 5 **reset ipsec** para volver a cargar la SRAM con la nueva configuración de IPsec. El mandato **reset ipsec** no afecta a ninguna configuración de IP. A continuación, utilice el mandato Talk 5 **reset ipv6** para restablecer IPv6 dinámicamente en el direccionador. Por otra parte, para restablecer cada componente, puede reiniciar el direccionador. Debe restablecer IPsec e IPv6, o bien reiniciar el direccionador para asegurarse de que vuelvan a cargarse las reglas de filtros. De lo contrario, es posible que su configuración no estuviera soportada correctamente en la interfaz. Consulte “Configuración y supervisión de la Seguridad de IP” en la página 387 y el mandato **reset ipv6** en el manual *Consulta de configuración y supervisión de protocolos Volumen 2* para obtener más información.

Tal como se muestra en la Figura 37 en la página 377, el túnel de IPsec 2 tiene un extremo en la interfaz 1 del direccionador B. Realice los siguientes pasos para configurar manualmente el direccionador B.

1. Cree el túnel de IPsec.
2. Cree un filtro de salida en la interfaz del direccionador que es el extremo del túnel de IPsec.
3. Cree reglas de control de acceso para los filtros de paquetes.
4. Restablezca IPsec.
5. Restablezca IPv6.

Creación del túnel de Seguridad de IP para el direccionador B

En el direccionador B, debe crearse el mismo túnel de IPsec que se creó para el direccionador A, el túnel de IPsec 2. La dirección IP local de este túnel en el direccionador B es 2000::B y la dirección IP remota es 2000::A. Todos los demás parámetros del túnel de IPsec deben coincidir con los que se especificaron para el direccionador A.

Configuración de filtros de paquetes para el direccionador B

Como hizo para el direccionador A, configure un filtro de paquetes de salida (*out-router-B*) en la interfaz 1, que es la interfaz del direccionador B que es el extremo del túnel de IPsec 1.

Configuración de las reglas de control de acceso de filtros de paquetes para el direccionador B

Configure una regla de control de acceso en *out-router-B* para pasar los paquetes de salida de la red 3000:1:: a IPSec para su proceso y transmisión a través del túnel de IPSec 2. Esta regla de control de acceso es de tipo I y S.

```
Packet-filter name [ ]? out-router-B
Packet-filter 'out-router-B' Config> add access
Enter type [E]? IS
Internet source [0::0]? 3000:1::
Prefix Length [64]? 64
Internet destination [0::0]? 1000:1::
Prefix Length [64]? 64
Enter IPsec Tunnel ID [1]? 2
Packet-filter 'out-router-B' Config>
```

Para *out-router-B*, cree una regla de control de acceso inclusiva, que permita a los paquetes ya procesados por IPSec pasar a través del túnel de IPSec 2.

```
Packet-filter 'out-router-B' Config> add access
Enter type [E]? I
Internet source [0::0]? 2000::B
Prefix Length [64]? 64
Internet destination [0::0]? 2000::A
Prefix Length [64]? 64
Packet-filter 'out-router-B' Config>
```

Para *out-router-B*, cree una regla comodín inclusiva de control de acceso, si desea que los paquetes que no coincidan con ninguna de las dos reglas de control de acceso pasen, en vez de eliminarlos; por ejemplo, el tráfico que no va destinado al túnel de IPSec 2.

Restablecimiento de la Seguridad de IP y de IPv6 en el direccionador B

Antes de que la función de IPSec funcione y los filtros se activen, debe restablecer IPSec e IPv6. Utilice el mandato `talk 5 reset IPSec` para restablecer IPSec y IPv6. Consulte “Restablecimiento de la Seguridad de IP y de IP en el direccionador A” en la página 408 para obtener información acerca del restablecimiento de IPSec. Después de restablecer IPSec, utilice el mandato `talk 5 reset IPv6` para restablecer IPv6. Como alternativa, puede reiniciar el direccionador para restablecer cada componente.

Ejemplo: configuración de un túnel de Seguridad de IP con ESP

Tenga en cuenta que este ejemplo sólo muestra la configuración del túnel de IPSec, no de los filtros de paquetes.

Acceso al entorno de Intercambio de claves de Internet (IPv4)

```
IPV6-IPsec config>add tun
Tunnel ID or Tunnel Name [ ]? 2
Tunnel Lifetime, in minutes (0-525600) [46080]?
Tunnel Encapsulation Mode (TUNN or TRANS) [TUNN]?
Tunnel Policy (AH,ESP,AH-ESP,ESP-AH) [ESP]?
Local IP Address [0::0]? 2000::A
Local Encryption SPI (256-65535) [256]?
Local Encryption Algorithm (DES-CBC,CDMF,3DES, NULL) [DES-CBC]?
Do you wish to change the Local Encryption Key? (Yes or [No]):
Additional Padding for Local Encryption (0-120) [0]?
Do you wish to use local ESP authentication? [Yes]:
Remote IP Address [0::0]? 2000::B
Remote Encryption SPI (1-65535) [256]?
Remote Encryption Algorithm (DES-CBC,CDMF) [DES-CBC]?
Do you wish to change the Remote Encryption Key? (Yes or [No]):
Do you wish to perform verification of remote encryption padding? [No]:
Do you wish to use remote ESP authentication? [No][No]:
Do you wish to enable this tunnel? [Yes]:
IPV6-IPsec config>
```

Ejemplo: configuración de un túnel de Seguridad de IP con ESP y ESP-NULL

Tenga en cuenta que la autenticación es obligatoria.

```
IPV6-IPsec config>add tun
Tunnel ID or Tunnel Name [ ]? 2
Tunnel Lifetime, in minutes (0-525600) [46080]?
Tunnel Encapsulation Mode (TUNN or TRANS) [TUNN]?
Tunnel Policy (AH,ESP,AH-ESP,ESP-AH) [ESP]?
Local IP Address [0::0]? 2000::A
Local Encryption SPI (256-65535) [256]?
Local Encryption Algorithm (DES-CBC,CDMF,3DES,NULL) [DES-CBC]? null
Additional Padding for Local Encryption (0-120) [0]?
Local ESP Authentication Algorithm (HMAC-MD5,HMAC-SHA) [HMAC-MD5]?
Local ESP Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Local ESP Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Remote IP Address [0::0]? 2000::B
Remote Encryption SPI (1-65535) [1234]?
Remote Encryption Algorithm (DES-CBC,CDMF,3DES,NULL) [NULL]?
Do you wish to perform verification of remote encryption padding? [No]:
Remote ESP Authentication Algorithm (HMAC-MD5,HMAC-SHA) [HMAC-MD5]?
Remote ESP Authentication Key (32 characters) in Hex (0-9,a-f,A-F):
Enter Remote ESP Authentication Key again (32 characters) in Hex (0-9,a-f,A-F):
Enable replay prevention? [No]:
Do you wish to enable this tunnel? [Yes]:
IPV6-IPsec config>
```

Supervisión de la Seguridad de IP manual (IPv4)

Esta sección explica cómo supervisar IPSec manual con IPv4. Describe cómo acceder al entorno de Intercambio de claves de Internet y los mandatos que hay disponibles.

Acceso al entorno de Intercambio de claves de Internet

Esta sección explica cómo utilizar el Protocolo de claves de Internet (IKE) con IPv4.

Para acceder al entorno de supervisión de IKE de la Seguridad de IP, entre la siguiente secuencia de mandatos en el indicador +:

```
+ feature ipsec
IPSP>ike
IKE>
```

Mandatos de supervisión del Intercambio de claves de Internet

Esta sección describe los mandatos de supervisión de IKE.

Tabla 50. Resumen de los mandatos de supervisión de IKE

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxiv.
Delete	Suprime dinámicamente las SA de fase 1 ISAKMP de un túnel específico, o todas las SA de fase 1.
List	Lista información acerca de las SA de fase 1 de un túnel específico, o todas las SA de fase 1.
Stats	Visualiza las estadísticas de un túnel.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiv.

Delete

Utilice el mandato IKE **delete** para suprimir dinámicamente una SA de fase 1 para un túnel o todas las SA de fase 1.

Sintaxis:

delete

tunnel

all

tunnel Especifica que va a suprimirse una SA de fase 1 para un túnel específico.

all Especifica que van a suprimirse todas las SA de fase 1.

Ejemplo: supresión de un túnel

```
PKI config>delete tunnel
Peer address [10.0.0.3]?
```

List

Utilice el mandato IKE **list** para visualizar información acerca de las SA de fase 1 de un túnel específico, o de todas las SA.

Sintaxis:

list tunnel

all

tunnel Especifica que va a visualizarse información para las SA de un túnel específico.

Mandatos de supervisión de IKE (Talk 5)

all Especifica que la información va a visualizarse para todas las SA.

Ejemplo: lista de información para todas las SA

```
IKE>list all
```

```
Phase 1 ISAKMP Tunnels for IPv4:
```

Peer Address	I/R	Mode	Auto	State	Auth
10.0.0.3	R	Aggr	N	QM_IDLE	pre-shared

```
IKE>LIST TUNNEL 10.0.0.3
```

```
Peer IKE address: 10.0.0.3
Local IKE address: 10.0.0.1
Role: Responder
Exchange: Aggr
Autostart: No
Oakley State: QM_IDLE
Authentication Method: Pre-shared Key
Encryption algorithm: des3
Hash function: md5
Diffie-Hellman group: 1
Refresh threshold: 85
Lifetime (secs): 15000
```

Stats

Utilice el mandato IKE **stats** para visualizar las estadísticas del túnel.

Sintaxis:

stats

tunnel

tunnel Visualiza información estadística acerca de las SA de un túnel.

Valores válidos: cualquier nombre de túnel o ID de túnel configurado.

Ejemplo: visualización de las estadísticas de SA de un túnel

```
IKE>stats
```

```
Peer address [10.0.0.3]?
```

```
Peer IP address.....: 10.0.0.3
Active time (secs)...: 187

In      Out
---    ---
Octets.....: 1229    1248
Packets.....: 14      16
Drop pkts.....: 0       1
Notifys.....: 6       0
Deletes.....: 0       0
Phase 2 Proposals....: 16     18
Invalid Proposals....: 0
Rejected Proposals....: 0
```


Acceso al entorno de la Infraestructura de clave pública (IPv4)

Esta sección explica cómo utilizar la Infraestructura de clave pública (PKI) con IPv4.

Para acceder al entorno de supervisión de PKI de la Seguridad de IP, entre la siguiente secuencia de mandatos en el indicador +:

```
+ feature ipsec
IPSP> pki
PKI>
```

Mandatos de supervisión de la Infraestructura de clave pública

Esta sección describe los mandatos de supervisión de la Infraestructura de clave pública (PKI).

Tabla 51. Resumen de los mandatos de supervisión de PKI

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxiv.
Cert-load	Carga un certificado en la SRAM de un direccionador.
Cert-req	Somete una petición de certificado a una CA.
Cert-save	Guarda un certificado en la antememoria para su posible uso en el futuro.
List certificate	Lista información acerca de un certificado.
List configured-servers	Visualiza información acerca de los servidores configurados.
Load certificate	Carga un registro que contiene el certificado de la SRAM en la antememoria de ejecución.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiv.

Cert-load

Utilice el mandato PKI **cert-load** para cargar un registro que contenga el certificado y la clave privada de la SRAM en la antememoria de certificado de ejecución.

Sintaxis:

cert-load

Ejemplo: carga de un registro de certificado de la SRAM en la antememoria

```
Enter type of certificate to be stored into SRAM:
  1)Root certificate;
  2)Box certificate with private key;
Select the certificate type (1-2) [2]?
Name []? test
mystr=1.1.1.1
Box certificate and private key saved into cache successfully
```

Cert-req

Utilice el mandato PKI **cert-req** para solicitar un certificado a una CA.

Sintaxis:

cert-req

Ejemplo: solicitud de un certificado a una CA

```
Enter the following part for the subject name
Country Name(Max 16 characters) []? us
Organization Name(Max 32 characters) []? ibm
Organization Unit Name(Max 32 characters) []? nhd
Common Name(Max 32 characters) []?
Key modulus size (512|768|1024)
[512]?
Certificate subject-alt-name type:
1--IPv4 Address
2--User FQDN
3--FQDN
Select choice [1]?
Enter an IPv4 addr) []? 1.1.1.1
Generating a key pair. This may take some time. Please wait ...
PKCS10 message successfully generated
Enter tftp server IP Address []? test
Bad address, try again
Enter tftp server IP Address []? 8.8.8.8
Remote file name (max 63 chars) [/tmp/tftp_pkcs10_file]?
Certificate request TFTP to remote host successfully.
```

Cert-save

Utilice el mandato PKI **cert-save** para guardar en la SRAM un registro que contenga el certificado y la clave privada.

Sintaxis:

cert-save

Ejemplo: guardar un registro de certificado en la SRAM

```
Enter type of certificate to be stored into SRAM:
1)Root certificate;
2)Box certificate with private key;
Select the certificate type (1-2) [2]?
SRAM Name for certificate and private key []? test
Load as default router certificate at initialization? [No]:
Private key TEST written into SRAM
Both Certificate and private key saved into SRAM successfully
```

List Certificate

Utilice el mandato PKI **list certificate** para visualizar información acerca de un certificado digital X.509.

Sintaxis:

list certificate

Ejemplo: lista de información de certificado

```
Router certificate
  Serial Number: 914034877
  Subject Name: /c=US/o=ibm/ou=nhd/cn=testip
  Issuer Name: /c=US/o=ibm/ou=nhd
  Subject alt Name: 1.1.1.1
  Key Usage: Sign & Encipherment
  Validity: 1999/1/19 23:24:27 -- 2002/1/19 23:54:27
```

List Configured-servers

Utilice el mandato PKI **list configured-servers** para visualizar información acerca de los servidores configurados.

Sintaxis:

list configured-servers

Ejemplo: lista de información acerca de los servidores configurados

- 1) Name: SERVER1
Type: LDAP
IP addr: 0.0.0.0
LDAP search timeout (secs): 0
LDAP retry interval (mins): 0
LDAP server port number: 0
LDAP version: 0
LDAP version: 0
Anonymous bind ?: y

- 2) Name: TEST
Type: TFTP
IP addr: 9.9.9.9

- 3) Name: TFTP
Type: TFTP
IP addr: 2.2.2.2

Load Certificate

Utilice el mandato PKI **load certificate** para cargar un certificado de la SRAM en la antememoria de ejecución.

Sintaxis:

load certificate

Mandatos de supervisión de Seguridad de IP (Talk 5)

Ejemplo: carga de un certificado en la antememoria

```
Enter the type of the certificate:
Choices: 1-Root CA Cert, 2-Router Cert
Enter (1-2): [2]?
Encoding format:
Choices: 1-DER 2-PEM
Enter (1-2): [1]?
Server info name []? test
Remote file name on tftp server (max 63 chars) [/tmp/default_file]? /tmp/test.cert

Attempting to load certificate file. Please wait ...
Router Certificate loaded into run-time cache
```

Acceso al entorno de supervisión de la Seguridad de IP (IPv4)

Para acceder al entorno de supervisión de la Seguridad de IP IPv4, escriba **t 5** en el indicador OPCON (*):

```
* t 5
```

A continuación, entre la siguiente secuencia de mandatos en el indicador +:

```
+ feature ipsec
IPSP>ipv4
IPV4-IPsec>
```

Mandatos de supervisión de la Seguridad de IP (IPv4)

Esta sección describe los mandatos de supervisión de la Seguridad de IP.

Tabla 52. Resumen de los mandatos de supervisión de la Seguridad de IP

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxiv.
Change tunnel	Cambia dinámicamente los valores de parámetros de configuración de túnel seguro
Delete tunnel	Suprime dinámicamente un túnel seguro.
Disable	Inhabilita dinámicamente todo el proceso de Seguridad de IP de manera segura (los paquetes coincidentes se eliminan), inhabilita todo el proceso de Seguridad de IP de manera no segura (los paquetes coincidentes pasan), o inhabilita un túnel seguro determinado.
Enable	Habilita dinámicamente todo el proceso de la Seguridad de IP, o habilita un túnel seguro.
List	Lista información global acerca de la Seguridad de IP, acerca de los túneles activos y definidos.
Reset	Restablece la Seguridad de IP o un túnel seguro. Este mandato recarga la configuración que se creó en Talk 6. El restablecimiento alterará temporalmente los valores de los parámetros configurados con Talk 5, sustituyéndolos por los configurados con Talk 6.
Set	Define dinámicamente el temporizador de antigüedad de la MTU de vía de acceso (PMTU).
Stats	Visualiza las estadísticas para todos los túneles o para un túnel activo.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiv.

Change Tunnel

Cambia dinámicamente un túnel seguro.

Sintaxis:

change tunnel ...

Vea la descripción del mandato **add tunnel** en “Mandatos de la configuración manual de la Seguridad de IP” en la página 393 para obtener una descripción de los parámetros.

Delete Tunnel

Utilice el mandato **delete** para suprimir dinámicamente un túnel seguro o todos ellos.

Sintaxis:

delete tunnel

tunnel-id
tunnel-name

all

tunnel-id Especifica el identificador del túnel de IPSec que se va a suprimir.

Valores válidos: 1 - 65535

Valor por omisión: 1

tunnel-name

Especifica el nombre del túnel de IPSec que se va a suprimir.

Valores válidos: cualquier nombre de túnel configurado

Valor por omisión: ninguno

all Especifica que se van a suprimir todos los túneles de IPSec que hay en esta interfaz.

Disable

Utilice el mandato **disable** para inhabilitar dinámicamente el protocolo de Seguridad de IP en todas las interfaces o en un único túnel.

Sintaxis:

disable

ipsec drop

ipsec pass

tunnel ...

ipsec drop

Inhabilita la seguridad de IP en el direccionador de manera segura. Se inhabilitarán todos los túneles de IPSec, pero se utilizará la información de túneles seguros en las reglas de filtros de paquetes para identificar los paquetes que coincidan con los filtros de paquetes de túnel de IPSec. Los paquetes coincidentes se eliminarán.

ipsec pass

Inhabilita la seguridad de IP en el direccionador de manera no segura. Se inhabilitarán todos los túneles de IPSec. Los paquetes que coincidan con los filtros de paquetes de túnel de IPSec se reenviarán como tráfico ordinario.

tunnel *tunnel-id* all

Inhabilita la seguridad de IP en un túnel específico o en todos los túneles.

tunnel-id

Especifica el identificador del túnel seguro que se va a inhabilitar.

Valores válidos: 1 - 65535

Valor por omisión: 1

all Todos los túneles.

Enable

Utilice el mandato **enable** para habilitar dinámicamente el protocolo de Seguridad de IP en todas las interfaces o en un único túnel. Debe habilitar IPSec en el direccionador de manera global antes de que se activen los túneles de IPSec habilitados individualmente.

Nota: IPSec no se puede habilitar dinámicamente si el direccionador se ha reiniciado con IPSec inhabilitado.

Sintaxis:

enable

ipsec
tunnel ...

ipsec

Habilita la seguridad de IP a través del direccionador.

tunnel *tunnel-id* | all

tunnel-id

Especifica el identificador del túnel seguro que se va a habilitar.

Valores válidos: 1 - 65535

Valor por omisión: 1

all Todos los túneles.

List

Utilice el mandato **list** para visualizar la configuración actual de la Seguridad de IP. Los túneles globales incluyen todos los túneles del direccionador, tanto los activos como los definidos. Todos los túneles incluye todos los configurados en esta interfaz, tanto los activos como los definidos. Los túneles activos son los que están activos actualmente; los túneles definidos están definidos, pero no activos.

Sintaxis:

list ...

all
global
tunnel

active *tunnel-id tunnel-name* all

defined *tunnel-id tunnel-name* all

Ejemplo 1: lista de todos los túneles activos

```
IPV6-IPsec>li tunnel ?
ACTIVE
DEFINED
IPsec>li tunnel active
Enter the Tunnel ID, Tunnel Name, or 'ALL' [ALL]? all

Tunnel Cache:

  ID      Local IP Addr  Remote IP Addr  Mode  Policy  Tunnel Expiration
  -----
    2      1.1.1.1        1.1.1.3        TRANS ESP *****
    1      1.1.1.1        2.1.1.1        TUNN  AH *****
```

Ejemplo 2: lista de un túnel activo que ha recibido el mensaje “packet too big (paquete demasiado grande)”

```
IPV6-IPsec>li tun act 1

Tunnel      Name      Mode Policy  Life  Replay      Tunnel      PMTU
ID          ID          ID          ID          ID          ID          ID          ID
-----
    1 tofran2      TUNN AH      46080  No  10:49 May 8 1998 1420 1

Local Information:

  IP Address: 2001:1::6101 2
  Authentication: SPI: 257 Algorithm: HMAC-MD5
  Encryption: SPI: ----- Encryption Algorithm: -----
  Extra Pad: ---
  ESP Authentication Algorithm: -----

Remote Information:

  IP Address: 2001.1..86
  Authentication: SPI: 257 Algorithm: HMAC-MD5
  Encryption: SPI: ----- Encryption Algorithm: -----
  Verify Pad?: ---
  ESP Authentication Algorithm: -----
```

1 La PMTU se visualiza como n/a si no se ha recibido ningún paquete demasiado grande.

2 Se trata de una dirección de IPv6. Si la versión de IP es IPv4, se visualiza un mensaje que define la gestión del bit DF: COPY, SET o CLEAR.

Ejemplo 3: lista de todos los túneles

```

IPV6-IPsec>li all

IPsec is ENABLED

IPsec Path MTU Aging Timer is 30 minutes

Defined Manual Tunnels for IPv4:
-----
   ID          Name          Local IP Addr  Remote IP Addr  Mode  State
-----
Defined Manual Tunnels for IPv6:
-----
ID=      1  Name= tofran2          Mode= TUNN   State= Enabled
Local IP address= 2001:1::6101
Remote IP address= 2001:1::86

Tunnel Cache for IPv4:
-----
   ID      Local IP Addr  Remote IP Addr  Mode  Policy  Tunnel Expiration
-----
Tunnel Cache for IPv6:
-----
ID=      1  Mode= TUNN  Policy= AH      Expiration= 10:49 May 8 1998
Local IP Address= 2001:1::6101
Remote IP Address= 2001:1::86

```

Reset

Utilice el mandato **reset** para restablecer dinámicamente la seguridad de IP en el direccionador o en un único túnel. Después de restablecer IPsec o los túneles, asegúrese de utilizar el mandato **reset IP** para restablecer la configuración de IP. Esto es necesario para volver a cargar la información de control de acceso, como los filtros de paquetes y sus reglas de control de acceso. Si no restablece IP, es posible que los filtros de paquetes y las reglas de control de acceso no den soporte a la nueva configuración de IPsec.

Rearrancar el direccionador es una posibilidad alternativa al uso de los mandatos **reset**. No obstante, el rearranque del direccionador lo desconecta de la red durante un tiempo, mientras que los mandatos **reset** sólo interrumpen las funciones IP.

Sintaxis:**reset**

```

ipsec
tunnel id-túnel nombre-túnel all

```

ipsec

Restablece la seguridad de IP en el 2216. La seguridad de IP se inhabilita temporalmente y después se reinicia. Mientras la seguridad de IP está inhabilitada, los paquetes normalmente gestionados por los túneles de IPsec se eliminan hasta que haya finalizado la operación de restablecimiento. El restablecimiento de la seguridad de IP no afecta a otras funciones del 2216. Este mandato activa la configuración de seguridad de IP que se creó utilizando Talk 6. La configuración de seguridad de IP de Talk 6 se graba encima de la configuración de Talk 5.

Mandatos de supervisión de Seguridad de IP (Talk 5)

tunnel

Restablece la seguridad de IP en un túnel específico. Si el túnel se inhabilita durante el restablecimiento, la configuración del túnel se reconstruirá a partir de la configuración de la SRAM, pero el túnel permanecerá inhabilitado tras el restablecimiento.

id-túnel

Especifica el identificador del túnel seguro que se debe restablecer.

Valores válidos: 1 - 65535

Valor por omisión: 1

nombre-túnel

Especifica el nombre del túnel seguro que se va a restablecer.

Valores válidos: cualquier nombre de túnel configurado

Valor por omisión: ninguno

all Todos los túneles.

Set

Define dinámicamente el temporizador de antigüedad de la MTU de vía de acceso (PMTU).

Sintaxis:

set path

path

Este parámetro define el tiempo, en minutos, que transcurrirá hasta que el 2216 defina de nuevo la MTU del túnel con su valor máximo.

Valor por omisión: 10 (0 significa que está inhabilitado)

Stats

Utilice el mandato **stats** para visualizar las estadísticas acerca de un túnel específico o de todos los túneles. Por ejemplo, el mandato **stats** muestra los paquetes enviados y recibidos.

Sintaxis:

stats

id-túnel

nombre-túnel

all

id-túnel

Especifica el identificador del túnel seguro.

Valores válidos: 1 - 65535

Valor por omisión: 1

nombre-túnel

Especifica el nombre de un túnel seguro que se ha configurado.

Valores válidos: cualquier nombre de túnel configurado

Valor por omisión: ninguno

all Visualiza estadísticas acerca de todos los túneles configurados en el 2216.

Ejemplo:

```

IPV6-IPsec>stats
Enter the Tunnel ID, Tunnel Name, or 'ALL' [ALL]? all

                                Global IPSec Statistics
Received:
  total pkts  AH packets  ESP packets  total bytes  AH bytes  ESP bytes
  -----
             0           0           0           0           0           0

Sent:
  total pkts  AH packets  ESP packets  total bytes  AH bytes  ESP bytes
  -----
             0           0           0           0           0           0

Receive Packet Errors:
  total errs  AH errors  AH bad seq  ESP errors  ESP bad seq
  -----
             0           0           0           0           0

Send Packet Errors:
  total errs  AH errors  ESP errors
  -----
             0           0           0

```

Supervisión de la Seguridad de IP manual (IPv6)

Esta sección explica cómo supervisar IPSec manual con IPv6. Describe cómo acceder al entorno de seguridad de IP y los mandatos que hay disponibles.

Acceso al entorno de supervisión de la Seguridad de IP

Para acceder al entorno de supervisión de la Seguridad de IP, escriba **t 5** en el indicador OPCON (*):

```
* t 5
```

A continuación, entre la siguiente secuencia de mandatos en el indicador +:

```
+ feature ipsec
IPSP>ipv6
IPV6-IPsec>
```

Mandatos de supervisión de la Seguridad de IP (IPv6)

Los mandatos de supervisión de la Seguridad de IP para IPv6 son los mismos que los utilizados para IPv4, a menos que se indique lo contrario. Consulte “Mandatos de supervisión de la Seguridad de IP (IPv4)” en la página 416 para ver una descripción de los mandatos. Entre los mandatos en el indicador IPV6-IPsec>.

Mandatos de supervisión de Seguridad de IP (Talk 5)

Utilización de la característica de Servicios diferenciados

Este capítulo describe cómo utilizar la característica de Servicios diferenciados (DiffServ), de tal manera que un direccionador pueda proporcionar un servicio favorito a los paquetes de datos IP adecuados. El direccionador, basándose en la información de la cabecera IP, clasifica los paquetes comparándolos con configuraciones predefinidas de la base de datos de política (creada con la característica de política). Consulte los detalles en “Utilización de la característica de política” en la página 307. Como resultado de ello, algunos paquetes pueden recibir un servicio favorito. Este capítulo se compone de las secciones siguientes:

- “Visión general de los Servicios diferenciados”
- “Terminología de los Servicios diferenciados” en la página 428
- “Configuración de los Servicios diferenciados” en la página 428

Visión general de los Servicios diferenciados

Actualmente, la mayoría de los dispositivos de reenvío instalados en una red IP proporcionan un servicio de mejor esfuerzo estándar a los paquetes de datos sobre la base de primero en llegar, primero en ser servido. Este método de entrega es adecuado para la mayor parte del tráfico, pero están apareciendo nuevas aplicaciones que requieren una transmisión más rápida y temprana de ciertos paquetes.

La característica de Servicios diferenciados (DiffServ) proporciona distintos niveles de servicio a los paquetes IP cuando un direccionador los procesa para su transmisión. DiffServ proporciona algunos paquetes con servicio favorito, reservando los recursos del sistema (almacenamientos intermedios) y los recursos de enlace (ancho de banda) para ellos. Una función de clasificador de DiffServ determina el tipo de servicio proporcionado a los paquetes IP, examinando diversos campos en la cabecera IP, por ejemplo, los rangos de las direcciones IP de origen y de destino y los números de puerto, el tipo de protocolo y el byte TOS de entrada. Para conseguir esto de manera escalable, los flujos individuales se agregan para formar corrientes. Las corrientes son las entidades mediante las cuales DiffServ gestiona el acceso a los almacenamientos intermedios y al ancho de banda. La Figura 38 muestra cómo procesa DiffServ los paquetes de una corriente.

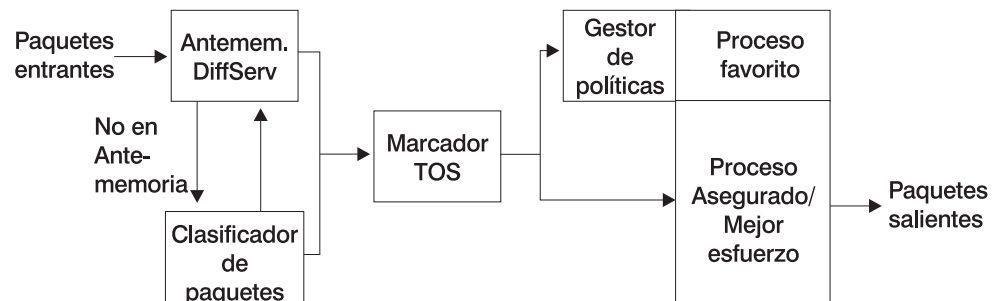


Figura 38. Vía de acceso de paquete de datos de DiffServ

Además del servicio de mejor esfuerzo tradicional, DiffServ proporciona los siguientes tipos de servicio:

Reenvío urgente (EF) El servicio de reenvío urgente representa la implementación de DiffServ de un servicio de calidad superior, y ambos términos se utilizan de manera indistinta en el texto siguiente. Este servicio garantiza una velocidad de transmisión específica y un retardo menor que el servicio de reenvío asegurado o de mejor esfuerzo. Si se desarrolla un tráfico excesivo, DiffServ eliminará el excedente. La cola del servicio superior proporciona el servicio EF y se muestra en la Figura 39 en la página 427 como cola EF.

Reenvío asegurado (AF) El servicio de reenvío asegurado representa la implementación de DiffServ de un servicio asegurado, y ambos términos se utilizan de manera indistinta en el texto siguiente. Este servicio garantiza una velocidad de transmisión específica, pero carece de garantía contra retardos. Si hay recursos desocupados, DiffServ puede enviar el exceso de tráfico a una velocidad superior. La cola AF/BE proporciona el servicio AF, que se muestra en la Figura 39 en la página 427.

Mejor esfuerzo (BE) Es el servicio de mejor esfuerzo estándar, que no proporciona garantías de servicio ni contra retardos. Debe encontrar un equilibrio entre la reserva de recursos para los servicios EF y AF, y dejar libres los recursos suficientes para que el tráfico de mejor esfuerzo reciba un servicio adecuado. La cola AF/BE proporciona el servicio BE, que se muestra en la Figura 39 en la página 427.

Los direccionadores locales crean y envían paquetes de control, de manera que también debe dejar libres los recursos suficientes para que reciban el servicio adecuado.

DiffServ se implementa actualmente en los enlaces PPP y Frame Relay y el sub-sistema RSVP puede utilizarlo. La Figura 38 en la página 425 muestra cómo se procesan los paquetes de una corriente de datos. Cuando un direccionador recibe el primer paquete de un flujo (suponiendo que esté designado para recibir el servicio de calidad superior), no existe ninguna indicación de que exista su categoría de servicio en la antememoria de vía de acceso rápida, por lo que el paquete se procesa con la vía de acceso lenta. DiffServ invoca una búsqueda de la base de datos de política para obtener los criterios de gestión de paquetes (política). La acción definida por la política se guarda en la antememoria de vía de acceso rápida. Cuando el direccionador reciba un paquete subsiguiente de este flujo, encontrará que ya existe una entrada en la antememoria de vía de acceso rápida para el flujo ya existente, de manera que se aplica su acción definida por la política y el paquete toma la vía de acceso rápida. Por consiguiente, los paquetes subsiguientes de este flujo recibirán el servicio de calidad superior.

La Figura 39 en la página 427 muestra la relación entre el gestor de política, la gestión de almacenamientos intermedios, las colas y el planificador: algunos componentes básicos que proporcionan distintos niveles de calidad de servicio.

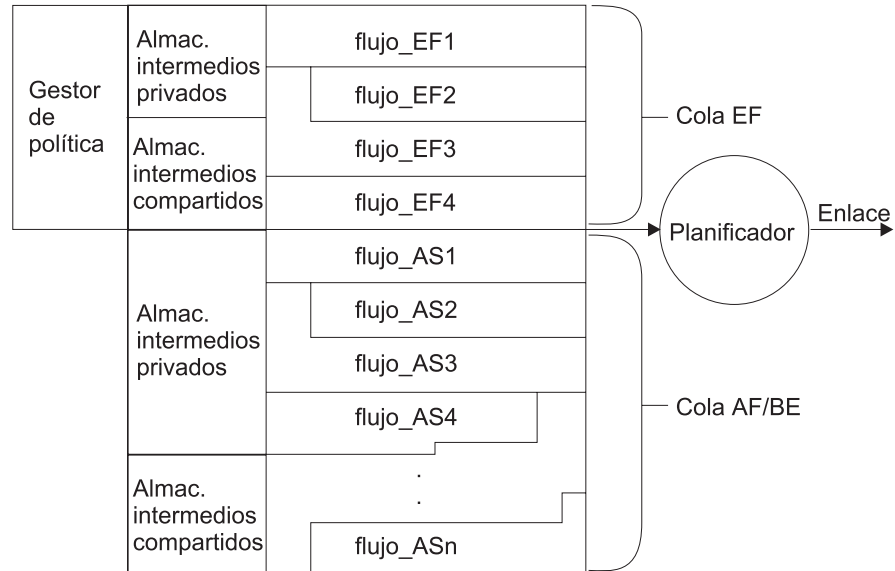


Figura 39. Relación entre los almacenamientos intermedios, las colas y el planificador

Los servicios de reenvío urgente (EF) y reenvío asegurado (AF) tienen características distintas, que están soportadas por tres funciones en el direccionador: (1) el gestor de política, (2) la gestión de almacenamientos intermedios y (3) el planificador. Estas funciones proporcionan un control de tráfico más sofisticado del que está disponible en un dispositivo de direccionador BE tradicional.

Si el tráfico requiere el proceso EF, debe eliminarse el exceso de tráfico. La función de *gestor de política* de DiffServ utiliza una muestra simbólica para examinar el tráfico EF y determinar si sobra un paquete. En caso afirmativo, el gestor de política elimina el paquete.

Si el gestor de política ha permitido que haya tráfico para AF, BE o EF, la función de *gestión de almacenamientos intermedios* basada en la velocidad lo procesará. Esta función asigna los almacenamientos intermedios de una agrupación privada para la interfaz, o de una agrupación compartida común para todas las interfaces. Utilice el mandato de configuración Talk 6 **set receive-buffers** (consulte el mandato set receive-buffers en el manual *Nways Multiprotocol Access Services Guía del usuario de software*) para especificar la cantidad total de espacio de almacenamiento intermedio físico disponible para una interfaz. Utilice el mandato Talk 6 **set interface** de DiffServ para definir el tamaño del almacenamiento intermedio de salida para las colas de calidad superior y aseguradas. Es el espacio de almacenamiento intermedio que DiffServ gestiona. (DiffServ gestiona dos agrupaciones distintas: una para la cola de calidad superior (EF) y la otra para la cola de reenvío asegurado (AF). Asegúrese de que el espacio de almacenamiento intermedio que especifique refleja la cantidad real de espacio de almacenamiento intermedio disponible en el sistema.) La gestión de almacenamientos intermedios determina si los almacenamientos intermedios de su agrupación privada de interfaz están disponibles para el paquete. En caso afirmativo, aceptará el paquete y lo pondrá en cola. En caso negativo, intentará asignar espacio de almacenamiento intermedio de la agrupación compartida y, si puede, pondrá el paquete en cola. Si no hay espacio de almacenamiento intermedio compartido disponible, la gestión de almacenamientos intermedios eliminará el paquete.

Utilización de los Servicios diferenciados

La función del *planificador* examina las colas de manera regular, quita los paquetes en cola de las colas, y los envía al adaptador de interfaz para su transmisión. Es un planificador de cola justa con reloj propio, que es una variante de las colas justas con pesos. Puede configurar los pesos del planificador y especificar la frecuencia con que el planificador examinará las colas.

Nota: Es posible configurar las opciones de DiffServ de tal manera que los recursos estén comprometidos o reservados en exceso, es decir, que los controladores del acondicionador de tráfico estén configurados como si hubiera más ancho de banda o almacenamientos intermedios de los que hay disponibles en realidad. DiffServ no da soporte al exceso de reserva.

Si una corriente de DiffServ queda desocupada (no se envía ningún paquete por la corriente por algún tiempo), el sistema reclama los recursos para que otras corrientes puedan utilizarlos. Si la corriente se reactiva, se le devolverán los recursos. Si los recursos ya no están disponibles debido a un exceso de reserva, DiffServ intentará reasignar los recursos periódicamente.

Después de haber utilizado la característica de política para configurar las políticas adecuadas, el primer paso para implementar DiffServ será utilizar el mandato DiffServ **set** para configurar las opciones que definen los recursos del sistema disponibles para DiffServ. A continuación, utilice el mandato **enable ds** para habilitar la característica DiffServ y el mandato **enable interface** para habilitar la interfaz de salida.

Terminología de los Servicios diferenciados

Se utilizan los siguientes términos al analizar DiffServ:

Antememoria de DiffServ

Esta antememoria contiene el perfil de tráfico y de servicio de los flujos IP activos más recientes a los que el direccionador da servicio.

Flujo

Secuencia de paquetes con la misma dirección y puerto de origen, protocolo IP, y dirección y puerto de destino.

Corriente

Una suma de flujos.

Interfaz virtual (VIF)

Para los enlaces Frame Relay, se considera que cada conexión DLCI es una interfaz virtual.

Configuración de los Servicios diferenciados

Los procedimientos siguientes proporcionan una descripción de alto nivel sobre cómo configurar DiffServ para proporcionar servicio favorito para los paquetes seleccionados. En primer lugar, acceda a la característica DiffServ:

1. En el indicador `*`, entre **talk 6**.
2. En el indicador `Config>`, entre **feature ds**. Se visualiza el indicador `DS config>` y se abre el diálogo de configuración.


```
* talk 6
Config>feature ds
DS config>
```

3. Habilite la característica DiffServ en un direccionador:

```
DS config>enable ds
DiffServ enabled
```

4. Habilite y defina los parámetros de interfaz:

```
DS config>set interface
Enter Diffserv Interface number [0]? 2
Set Premium Queue Bandwidth (%) (1 - 99) [20]?
    Assured Queue Bandwidth (%) = 80
Configure Advanced setting (y/n)? [No]: no
Accept input (y/n)? [Yes]:
```

Nota: Si especifica no en la solicitud Configure Advanced setting, se utilizarán los parámetros por omisión para las colas Premium Queue y Assured/BE.

```
Configure Advanced setting (y/n)? [No]: yes
Set Premium Queue Weight (%) (20 - 99) [90]?
    Assured Queue Weight (%) = 10
EGRESS BufSize for Premium Queue (in bytes) (550 - 16500) [5500]?
Max EGRESS QoS Allocation for Premium Queue (%) (1 - 99) [95]?
EGRESS BufSize for Assured/BE Queue (in bytes) (5500 - 140800) [27500]?
Max EGRESS QoS Allocation for Assured/BE Queue (%) (1 - 99) [80]?
```

En este ejemplo se proporcionan unos pesos de 20 por ciento de ancho de banda de línea y 90 por ciento del planificador a la cola EF. El tamaño del almacenamiento intermedio de salida para la cola EF es 5500 (en bytes), del que un 95 por ciento puede asignarse a las corrientes QOS. El tamaño del almacenamiento intermedio de salida para la cola AF/BE es 27500 (en bytes), del que un 80 por ciento puede asignarse a las corrientes QOS.

5. Cuando haya terminado de habilitar DiffServ en los direccionadores y de definir los parámetros de interfaz, pulse **Control-P** para regresar al indicador *.

Después de habilitar DiffServ y de definir los parámetros de interfaz, debe volver a iniciar o a cargar el dispositivo para activar DiffServ. Para obtener más detalles sobre la especificación de mandatos de DiffServ, consulte “Configuración y supervisión de la característica de Servicios diferenciados” en la página 431.

Configuración y supervisión de la característica de Servicios diferenciados

Este capítulo describe los mandatos proporcionados por los Servicios diferenciados (DiffServ) para configurar direccionadores e interfaces para proporcionar servicio favorito para los paquetes de datos seleccionados. Incluye las secciones siguientes:

- “Acceso al indicador de configuración de los Servicios diferenciados”
- “Mandatos de configuración de los Servicios diferenciados”
- “Acceso al entorno de supervisión de los Servicios diferenciados” en la página 436
- “Mandatos de supervisión de los Servicios diferenciados” en la página 437

Acceso al indicador de configuración de los Servicios diferenciados

Para entrar los mandatos de configuración de DiffServ:

1. Entre **talk 6** en el indicador OPCODE (*).
2. Entre **feature ds** en el indicador Config>.

Aparece el indicador DS Config>. Ahora puede entrar los mandatos de configuración de DiffServ.

Mandatos de configuración de los Servicios diferenciados

Estos mandatos le permiten configurar las opciones de DiffServ, que designan el servicio favorito para los paquetes de datos seleccionados. La Tabla 53 resume los mandatos de configuración de DiffServ y el resto de esta sección los describe con detalle. Entre los mandatos en el indicador DS Config>. Entre el mandato y las opciones en una línea, o bien entre sólo el mandato y después responda a los indicadores. Para ver una lista de las opciones de mandato válidas, entre el mandato con un signo de interrogación en lugar de especificar opciones.

Tabla 53. Mandatos de configuración de DiffServ

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxiv.
Delete	Suprime un registro de configuración de DiffServ de la SRAM de un direccionador.
Disable	Inhabilita DiffServ en un direccionador o en una interfaz de salida específica.
Enable	Habilita DiffServ en un direccionador o en una interfaz de salida específica.
List	Visualiza la información acerca del sistema DiffServ y los valores relativos a la interfaz de un direccionador.
Set	Especifica los valores de un direccionador relativos a DiffServ.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiv.

Delete

Utilice el mandato **delete** para suprimir un registro de configuración del sistema de DiffServ o un registro de interfaz de la SRAM de un direccionador.

Sintaxis: `delete ds
interface`

ds Suprime el registro de configuración del sistema de DiffServ perteneciente al direccionador.

Ejemplo:

```
DS Config> delete ds
Diffserv system config record deleted
```

interface

Le solicita el número de interfaz que se va a suprimir.

Ejemplo:

```
DS Config> delete interface
Enter Diffserv Interface number to delete [0]? 3
Diffserv interface config record deleted
```

Disable

Utilice el mandato **disable** para inhabilitar la función DiffServ en un direccionador o en una interfaz de salida específica.

Sintaxis: `disable ds
interface`

ds Inhabilita la función DiffServ del direccionador.

Ejemplo:

```
DS Config> disable ds
DiffServe feature disabled
```

interface

Le solicita el número de la interfaz que se va a inhabilitar.

Ejemplo:

```
DS Config> disable interface
Enter Interface number [0]? 2
DiffServe interface disabled
```

Enable

Utilice el mandato **enable** para habilitar la función DiffServ en un direccionador o en una interfaz de salida específica.

Sintaxis: `enable ds
interface`

ds Habilita la función DiffServ del direccionador.

Ejemplo:

```
DS Config> enable ds
DiffServe feature enabled
```

interface

Le solicita el número de la interfaz que se va a habilitar.

Ejemplo:

```
DS Config> enable interface
Enter Interface number [0]? 2
DiffServe interface enabled
```

Nota: DiffServ sólo se puede habilitar en los enlaces PPP y Frame Relay.

List

Utilice el mandato **list** para visualizar información acerca del sistema DiffServ y los valores relativos a la interfaz de un direccionador.

Sintaxis: `list` all
 ds
 interface

all Visualiza la información acerca de la configuración de DiffServ y de la interfaz de un direccionador.

ds Visualiza la configuración de DiffServ de un direccionador.

Ejemplo:

```
DS Config> list ds
```

System Parameters:

```
DiffServ:           ENABLED
Packet_size:        550
Min BE Alloc (%):   10
Min CTL Alloc (%):  5
Number_of_Q:        2
```

interface

Visualiza las interfaces en un direccionador, su estado de habilitación/inhabilitación de DiffServ y los parámetros para cada interfaz y cada cola.

Ejemplo:

```
DS Config> list interface
```

```
----- Premium ----- Assured -----
Net If   Status  NumQ  Bwdth  Wght  OutBuf  MaxQos  Bwdth  Wght  OutBuf  MaxQos
Num                                     (%)   (%) (bytes)  (%)   (%)   (%) (bytes)  (%)
-----
```

Net If Num	Status	NumQ	Bwdth (%)	Wght (%)	OutBuf (bytes)	MaxQos (%)	Bwdth (%)	Wght (%)	OutBuf (bytes)	MaxQos (%)
2	PPP Enabled	2	20	90	5500	95	80	10	27500	80
3	PPP Enabled	2	20	90	5500	95	80	10	55000	80

Set

Utilice el mandato **set** para definir el sistema Diffserv y los parámetros relativos a la interfaz de un direccionador.

Sintaxis: `set` `be-alloc-min`
 `ctl-alloc-min`
 `interface`
 `pkt-size`

be-alloc-min

Especifica el porcentaje mínimo del espacio total de almacenamiento intermedio de salida para asignar el servicio de mejor esfuerzo.

Valor por omisión: 10

Ejemplo:

```
DS Config> set be-alloc-min
Enter Minimum percent output BW allocated to BE service (10 - 50) [10]?
```

ctl-alloc-min

Especifica el porcentaje mínimo del espacio total de almacenamiento intermedio de salida para asignar el servicio de control de red.

Valor por omisión: 5

Ejemplo:

```
DS Config> set ctl-alloc-min
Enter Minimum percent output BW allocated to CTL service (5 - 20) [5]?
```

interface

Especifica la interfaz para habilitar DiffServ y le solicita los parámetros específicos de la interfaz.

Queue bandwidth Especifica el porcentaje del enlace de salida que debe utilizarse para la cola de calidad superior. El porcentaje restante se utiliza para el valor de cola asegurada.

Valor por omisión: 20

Queue weight Especifica el porcentaje de tiempo que el planificador supervisa la cola de calidad superior. El porcentaje restante se utiliza para el valor de cola asegurada. El peso de cola es, por omisión, del 90 por ciento para que el planificador reaccione con rapidez al tráfico EF.

Valor por omisión: 90

Egress buffer size Especifica la cantidad de datos (en bytes) que pueden ponerse en cola en las colas de calidad superior y asegurada.

Para la cola de calidad superior, este parámetro controla la cantidad de datos (en bytes) que pueden ponerse en la cola de calidad superior. Un valor excesivamente grande para este parámetro podría causar un elevado retardo de puesta en cola para el tráfico de calidad superior. Por ejemplo, si se define como 25 Kbytes y la velocidad del enlace de salida es 1,5 Mbps (velocidad T1), existe un retardo potencial de puesta en cola de 133 mseg (25000 bytes * 8 bits/byte)/1500000 bps, ó 0,133 seg (133 milisegundos). Un valor

demasiado pequeño para este parámetro podría imposibilitar las pequeñas ráfagas de almacenamiento intermedio. Por ejemplo, si se define como 2 Kb, implica que no habrá almacenamiento intermedio suficiente para una ráfaga de 2 paquetes de 1500 bytes (dado que requieren 3000 bytes de espacio de almacenamiento intermedio).

Como compromiso entre estos dos extremos, el valor por omisión es de 5500 bytes, que es diez veces el tamaño de paquete por omisión, que es de 550.

Valor por omisión: 5500 (cola de calidad superior).

Para la cola asegurada, este parámetro controla la cantidad de datos (en bytes) que pueden ponerse en la cola asegurada. Las consideraciones sobre este valor de parámetro son las mismas que para la cola de calidad superior, salvo que el tráfico de la cola asegurada no tiene requisitos de retardo muy estrictos. Es más probable que el tráfico de la cola asegurada consista en flujos TCP, que tienen la peculiaridad de tener muchas ráfagas. Debido a ello, es preciso definir un espacio de almacenamiento intermedio suficiente para acomodar las ráfagas de varios flujos.

Un valor de 27500, que equivale a cincuenta veces el tamaño de paquete por omisión, que es de 550.

Valor por omisión: 27500 (cola asegurada)

Egress QoS allocation Especifica la cantidad del valor del tamaño de almacenamiento intermedio de salida (como porcentaje) que todas las corrientes de DiffServ pueden reservar. El porcentaje restante se utiliza para el tamaño mínimo de la agrupación compartida.

Valor por omisión: 95 (cola de calidad superior)

Valor por omisión: 80 (cola asegurada)

Ejemplo:

```
DS Config> set interface
Enter Diffserv Interface number [0]? 2

DiffServ Interface enabled

Set Premium Queue Bandwidth (%) (1 - 99) [20]?
  Assured Queue Bandwidth (%) = 80

Configure Advanced setting (y/n)? [No]: y

Set Premium Queue Weight (%) (20 - 99) [90]?
  Assured Queue Weight (%) = 10

EGRESS BufSize for Premium Queue (in bytes) (550 - 16500) [5500]?
Max EGRESS QoS Allocation for Premium Queue (%) (1 - 99) [95]?

EGRESS BufSize for Assured/BE Queue (in bytes) (5500 - 140800) [27500]?
Max EGRESS QoS Allocation for Assured/BE Queue (%) (1 - 99) [80]?

      DiffServ Interface: ENABLED
PREMIUM Queue Bandwidth (%) =                20
PREMIUM Queue Weight (%) =                   80
PREMIUM Queue EGRESS BufSize in bytes =      5500
PREMIUM Queue Max EGRESS QoS allocation (%) =  95
ASSURED/BE Queue Bandwidth (%) =              80
ASSURED/BE Queue Weight (%) =                20
ASSURED/BE Queue EGRESS BufSize in bytes =   27500
ASSURED/BE Queue Max EGRESS QoS allocation (%) = 80
Accept input (y/n)? [Yes]:
```

pkt-size

Especifica el tamaño de paquete medio del flujo de tráfico (en bytes). Esto permite a DiffServ determinar el espacio de almacenamiento intermedio disponible en las interfaces de entrada y salida. Si esto se cambia, es preciso reiniciar el direccionador y revisar y modificar los valores del mandato DiffServ **set interface**, si es necesario.

Valor por omisión: 550

Ejemplo:

```
DS Config> set pkt-size
Average packet size (64 - 64000) [550]?
```

Acceso al entorno de supervisión de los Servicios diferenciados

La parte de consola de la característica DiffServ permite ver y gestionar los valores relativos a DiffServ. Para acceder al entorno de supervisión de DiffServ, entre **talk 5** en el indicador OPCON (*):

```
* t 5
```

A continuación, entre el siguiente mandato en el indicador +:

```
+ feature ds
DS Console>
```


Mandatos de supervisión de los Servicios diferenciados

Estos mandatos le permiten ver los valores relativos a DiffServ. La Tabla 54 resume los mandatos de supervisión de DiffServ, que se describen en el resto de esta sección. Entre los mandatos en el indicador DS Console>. Entre el mandato y las opciones en una línea, o bien entre sólo el mandato y después responda a los indicadores. Para ver una lista de las opciones de mandato válidas, entre el mandato con un signo de interrogación en lugar de especificar opciones.

Tabla 54. Mandatos de supervisión de DiffServ

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxiv.
Clear	Borra las estadísticas para una corriente entre un par específico de interfaces de entrada y salida.
DScache	Borra o visualiza información en la antememoria de DiffServ de un direccionador.
List	Visualiza la información acerca del sistema DiffServ y los valores relativos a la interfaz de un direccionador.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiv.

Clear

Utilice el mandato **clear** para borrar las estadísticas de una corriente entre un par específico de interfaces de entrada y de salida.

Sintaxis: `clear` `stream-stats`

Ejemplo:

```
DS Console> clear stream-stats
Incoming Network number : 0
Outgoing Network number : 2
IN Net 0 DiffServ not enabled.
Net 0->2 stream stats cleared at sysclock 85327 Second.
```

DScache

Utilice el mandato **dscache** para borrar o visualizar información en la antememoria de DiffServ de un direccionador.

Sintaxis: `dscache` `actions`
`clear`
`nexthop`
`order`
`stats`

actions

Visualiza las acciones que deben realizarse para los paquetes enviados desde el origen IP especificado al destino IP especificado, y el ID de corriente de DiffServ, si lo hay.

Mandatos de supervisión de DiffServ (Talk 5)

Ejemplo:

```
DS Console> dscache actions
Source Address to list []?
Destination Address to list []?
Source      Destination    Pro ProtocolInf Net TosIn/Out Action StrmID
10.1.100.1  9.1.140.1     1 T:x08 C:x00  0 x00->x15 PASS 85
9.1.140.1   10.1.100.1   1 T:x00 C:x00  1 x00->x15 PASS null
```

clear

Especifica el borrado de toda la antememoria de DiffServ.

nexthop

Visualiza la dirección IP nexthop.

Ejemplo:

```
DS Console> dscache nexthop
Source Address to list []? 5.0.13.248
Destination Address to list []? 5.0.11.249
Source      Destination    Pro ProtocolInf Net Tos NextHop
5.0.13.248  5.0.11.249    17 1031> 1031 0 x00 5.0.61.7 (PPP/1)
5.0.13.248  5.0.11.249    17 1032> 1032 0 x00 5.0.61.7 (PPP/1)
5.0.13.248  5.0.11.249    17 1033> 1033 0 x00 5.0.67.1 (PPP/1)
```

order

Visualiza el orden en que han llegado los paquetes.

Ejemplo:

```
DS Console> dscache order
Order Source      Destination    Pro ProtocolInf Net Tos
1 5.0.16.246      5.0.13.248    1 T:x03 C:x03 2 x00
2 5.0.13.248      5.0.16.246    17 4000> 5678 0 x00
3 5.0.16.246      5.0.13.244    1 T:x03 C:x03 1 x00
4 5.0.13.248      5.0.15.243    17 123> 123 0 x00
```

stats

Visualiza las estadísticas de los paquetes enviados desde el origen IP especificado al destino IP especificado.

Ejemplo:

```
DS Console> dscache stats
Source Address to list []? 5.0.13.248
Destination Address to list []? 5.0.11.249
Source      Destination    Pro ProtocolInf Net Tos RxPkts RxBytes
5.0.13.248  5.0.11.249    17 1031> 1031 0 x00 432 444096
5.0.13.248  5.0.11.249    17 1032> 1032 0 x00 432 444096
5.0.13.248  5.0.11.249    17 1033> 1033 0 x00 437 459516
```

List

Utilice el mandato **list** para visualizar información acerca del sistema DiffServ y los valores relativos a la interfaz de un direccionador.

Sintaxis: `list` interface
queue
stream
vifs

interface

Lista las interfaces en un direccionador, su estado de habilitación/inhabilitación de DiffServ, sus asignaciones de almacenamiento intermedio de entrada y otros tipos de información.

- Net** Visualiza el número de interfaz.
- Status** Visualiza el estado de DiffServ.
- KB/s** Visualiza la velocidad del enlace en Kb por segundo.
- VirtTime** Visualiza la hora virtual utilizada por el planificador (indica n/a para los enlaces que no sean DiffServ, e indica 0 si no hay ningún paquete en proceso).
- InMax** Visualiza el tamaño máximo de almacenamiento intermedio configurado para el reenvío asegurado.
- InCurr** Visualiza la cantidad de espacio de almacenamiento intermedio que se utiliza actualmente para la corriente de entrada. Los almacenamientos intermedios contienen paquetes en proceso.
- InShar** Visualiza la cantidad de espacio de almacenamiento intermedio compartido para esta interfaz de salida.
- InMaxA** Visualiza la cantidad máxima de espacio de almacenamiento intermedio que puede asignarse a todas las corrientes de QoS como agregación.
- InCurA** Visualiza la cantidad de espacio de almacenamiento intermedio asignado para que lo utilice la corriente de entrada.
- NumI** Visualiza el número de corrientes de entrada.
- NumO** Visualiza el número de corrientes de salida.

Ejemplo:

```
DS Console> list interface
```

```
DiffServ interfaces:
```

Net	Status	KB/s	VirtTime	InMax	InCurr	InShar	InMaxA	InCurA	NumI	NumO
0	Disabled	1250	n/a	55000	550	49775	44000	5225	22	n/a
1	Disabled	1250	n/a	27500	0	27500	22000	0	20	n/a
2	Enabled	256	0	27500	0	27500	22000	0	20	3
3	Enabled	256	0	55000	0	55000	44000	0	20	3
4	Disabled	0	n/a	550000	0	550000	550000	0	20	n/a
5	Disabled	0	n/a	550000	0	550000	550000	0	20	n/a
6	Disabled	0	n/a	550000	0	550000	550000	0	20	n/a
7	Disabled	0	n/a	550000	0	550000	550000	0	20	n/a
8	Disabled	2000	n/a	27500	0	27500	22000	0	20	n/a
9	Disabled	0	n/a	550000	0	550000	550000	0	20	n/a

queue

Visualiza los pesos asignados a las colas de salida de DiffServ y el estado de asignación de almacenamiento intermedio de las interfaces de salida.

- Queued packets** Visualiza el número de paquetes que están puestos en cola actualmente (0 indica que no hay paquetes en cola).
- Svc Tag** Visualiza la siguiente hora virtual en que esta cola debe recibir servicio técnico.
- Weight** Visualiza el peso del planificador de esta cola.

Mandatos de supervisión de DiffServ (Talk 5)

out_max_alloc Visualiza la cantidad máxima de espacio de almacenamiento intermedio que puede asignarse a una corriente DiffServ.

out_curr_alloc Visualiza la cantidad actual de espacio de almacenamiento intermedio asignado.

out_max_buff Visualiza la cantidad máxima de espacio de almacenamiento intermedio para esta cola.

out_curr_buff Visualiza la cantidad actual de espacio de almacenamiento intermedio asignado que se utiliza para los paquetes.

out_share_buff Visualiza la cantidad de espacio de almacenamiento intermedio que hay actualmente en la agrupación compartida.

Ejemplo:

```
DS Console> list queue
OUT Network number : 1
```

```
Premium Queue:
  Queued packets: 0
  Svc Tag:       4294967295
  Weight: 20
  out_max_alloc: 5225 (Bytes)
  out_curr_alloc: 0 (Bytes)
  out_max_buff:  5500 (Bytes)
  out_curr_buff: 0 (Bytes)
  out_share_buff: 5500 (Bytes)
```

```
Assured Queue:
  Queued packets: 0
  Svc Tag:       4294967295
  Weight: 80
  out_max_alloc: 22000 (Bytes)
  out_curr_alloc: 4125 (Bytes)
  out_max_buff:  27500 (Bytes)
  out_curr_buff: 0 (Bytes)
  out_share_buff: 23375 (Bytes)
```

stream

Visualiza información acerca de las corrientes.

Id Número de identificación de la corriente

t Tipo de corriente

D Corriente de DiffServ

B Corriente de mejor esfuerzo

C Corriente de control de red

R Corriente de RSVP

I/o q Tipo de cola

q1 Cola de calidad superior

q2 Cola asegurada/BE

allo/cur(K) Espacio total de almacenamiento intermedio (en kilobytes) asignado por esta corriente.

tot pkt Total de paquetes recibidos por esta corriente para su transmisión.

tot Kby Total de kilobytes recibidos por esta corriente para su transmisión.

- pkt snt** Total de paquetes enviados por esta corriente.
- Kby snt** Total de kilobytes enviados por esta corriente.
- ovr snt** Número de paquetes enviados utilizando almacenamientos intermedios compartidos.
- buf drp** Número de paquetes eliminados de esta corriente porque no había espacio de almacenamiento intermedio disponible.
- policed** Número de paquetes eliminados por el gestor de política en la cola de calidad superior.

Ejemplo:

```
DS Console> list stream
Incoming Network number : 0
Outgoing Network number : 2
At interface 0, 22 in-streams; clock=904 sec.
Streams from net 0 to net 2:
  Id  t I/o q  allo/cur(K)  tot pkt  tot Kby  pkt snt  Kby snt  ovr snt  buf drp  policed
  ---  -  -  -  -  -  -  -  -  -  -  -  -
(policy name)
  85  D  in   5.2/  0.0   82384   43828   48653   25883    0      0
      o-q1 5.2/  1.1           48653   25883    0      0      732

(-)
  55  B  in   0.0/  0.0     0      0      0      0      0      0
      o-q2 2.8/  0.0           263     21      0      0      0

(-)
  44  C  in   0.0/  0.0     0      0      0      0      0      0
      o-q2 1.4/  0.0           79      6      0      0      0
```

vifs

Visualiza información acerca de las interfaces virtuales Frame Relay.

Ejemplo:

```
DS Console> list vifs 1

DiffServ virtual interface for dlci: 17
  Status: Inactive - no packets queued for transmission
  CIR: 64000 (bits/sec)
  Virtual Time: 0
  Service Tag: 0

DiffServ virtual interface for dlci: 16
  Status: Inactive - no packets queued for transmission
  CIR: 64000 (bits/sec)
  Virtual Time: 0
  Service Tag: 0
```

Mandatos de supervisión de DiffServ (Talk 5)

Utilización de Layer 2 Tunneling (L2TP, PPTP, L2F)

Layer 2 Tunneling (L2T) se compone de los protocolos de túnel L2TP, L2F y PPTP.

Layer 2 Tunneling Protocol (L2TP) es un protocolo de seguimiento estándar IETF para los túneles de PPP a través de una red de paquetes como UDP/IP. L2TP está orientado a la conexión.

Layer 2 Forwarding (L2F) y Point to Point Tunneling Protocol (PPTP) son protocolos informativos IETF para los túneles de PPP a través de una red IP.

Visión general de L2TP

L2TP permite que muchos dominios de protocolo independientes y autónomos compartan una infraestructura de acceso común incluyendo módems, Servidores de acceso y direccionadores RDSI. L2TP permite establecer túneles de la capa de enlace PPP, por ejemplo, HDLC y HDLC asíncrono. Utilizando estos túneles, es posible disociar la ubicación del servidor de marcación con el que se ha establecido contacto, de la ubicación que proporciona acceso a la red.

Tradicionalmente, el servicio de red de marcación en Internet se proporciona sólo para las direcciones IP registradas. L2TP define una nueva clase de aplicación de marcación virtual que permite varios protocolos y direcciones IP no registradas en Internet. Esta clase de aplicación de red es útil para dar soporte a marcaciones de direcciones privadas IP, IPX y AppleTalk a través de PPP en una infraestructura de Internet existente.

El soporte de aplicaciones de marcación virtual multiprotocolo es ventajoso para los usuarios finales, empresas y proveedores de servicio de Internet, porque permite compartir inversiones significativas en la infraestructura nuclear y de acceso, y permite a los usuarios utilizar las llamadas locales al acceder a los servicios.

L2TP también permite el uso seguro de inversiones existentes en aplicaciones de protocolos que no sean IP en la infraestructura de Internet existente.

La Figura 40 en la página 444 muestra un ejemplo de red L2TP utilizando RDSI. La red puede utilizar cualquier tipo de medios entre el Concentrador del acceso a red L2TP (LAC) y el Servidor de red L2TP (LNS).

Términos de L2TP

Se utilizan los siguientes términos al describir L2TP:

Par de valores de atributos (AVP)

Método uniforme de codificar tipos y textos de mensaje. Este método maximiza la extensibilidad, al tiempo que permite la interoperatividad de L2TP.

Concentrador de acceso a L2TP (LAC)

Dispositivo conectado a una o más líneas RDSI o PSTN (red telefónica de servicio público) que sean capaces de gestionar la operación de PPP y el protocolo L2TP. El LAC implementa los medios a través de los cuales opera

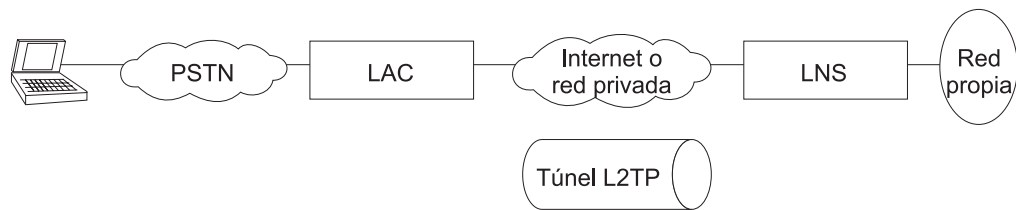


Figura 40. Ejemplo de red L2TP

L2TP. L2TP pasa el tráfico a uno o más Servidores de red L2TP (LNS). L2TP puede establecer un túnel para cualquier protocolo transportado por la red PPP.

Servidor de red L2TP (LNS)

Un LNS opera en cualquier plataforma que pueda ser una estación final PPP. El LNS gestiona el lado del servidor del protocolo L2TP. Dado que L2TP sólo se basa en el medio a través del cual llegan los túneles L2TP, el LNS sólo puede tener una única interfaz LAN o WAN; no obstante, todavía es posible terminar las llamadas que lleguen desde cualquier interfaz PPP soportada por un LAC.

Servidor de acceso a red (NAS)

Dispositivo que proporciona a los usuarios un acceso temporal y bajo demanda a la red. Este acceso es punto a punto, utilizando líneas PSTN o RDSI.

Sesión (Llamada)

L2TP crea una sesión cuando se intenta una conexión PPP de extremo a extremo entre un usuario que utiliza la marcación y el LNS. Los datagramas de la sesión se envían a través del túnel entre el LAC y el LNS. El LNS y el LAC mantienen la información de estado para cada usuario conectado a un LAC.

Túnel

Un túnel se define mediante un par LNS-LAC. El túnel transporta datagramas PPP entre el LAC y el LNS. Un único túnel puede actuar de multiplexor de muchas sesiones. Una conexión de control, que opera a través del mismo túnel, controla el establecimiento, la liberación y el mantenimiento de todas las sesiones y del túnel propiamente dicho.

Características soportadas

L2TP se ejecuta a través de UDP/IP y da soporte a las funciones siguientes:

- Túneles de clientes de marcación de entrada de un único usuario
- Túneles de pequeños direccionadores como, por ejemplo, un direccionador con una única ruta estática que se configura según un perfil de usuario autenticado.
- Las llamadas pueden iniciarse desde el LAC al LNS (de entrada), desde el LNS al LAC (de salida) o por cualquiera de los similares (ambas). Las llamadas de salida pueden ser *fijas* (siempre activas) o una sesión de túnel L2 según la demanda.
- Varias llamadas por túnel.
- Autenticación de proxy para PAP, CHAP y MS-CHAP.

- LCP de proxy.
- Reinicio de LCP, en caso de que no se utilice el LCP de proxy en el LAC.
- Autenticación de punto final de túnel.
- AVP oculto para transmitir una contraseña PAP de proxy.
- Túneles utilizando una tabla de consulta de rhelm local (es decir, usuario@rhelm).
- Túneles utilizando la consulta de nombres de usuario PPP en el subsistema AAA.
- Gestión de túneles L2TP utilizando SNMP. Consulte “SNMP Management” en el manual *Consulta de configuración y supervisión de protocolos Volumen 1*.

Nota: Los túneles rhelm requieren el uso de nombres de usuario en el formato *nombre@rhelm*. De esta forma, los túneles requieren que el software examine dos tablas para resolver el destino hacia el que se envía al usuario de marcación de entrada a través de un túnel. La ventaja de utilizar este método de generación de túneles es que sólo tiene que definir el rhelm, y los nombres de usuario que coincidan con el rhelm se enviarán a través del túnel al mismo lugar de destino.

Los túneles basados en el usuario se resuelven en una única tabla. Permiten la granularidad de transportar cada usuario por túnel a un destino exclusivo.

- BRS para un LNS (como punto final PPP).
- La capacidad de utilizar el mandato **delete interface** para suprimir los dispositivos L2TP.
- La capacidad para reconfigurar dinámicamente los dispositivos L2TP.
- El establecimiento de un procedimiento de poner en secuencia y poner en cola, así como de la retransmisión y el flujo de un canal de control. L2TP también realizar el control de flujo, puesta en secuencia y puesta en cola en los canales de datos.
- La capacidad de fijar el puerto UDP L2TP (1701) para que pueda establecer filtros de Seguridad de IP basados en el puerto UDP.
- Un cliente de direccionador L2TP. El cliente de direccionador L2TP es del modelo “iniciado por el cliente” (también conocido como túneles voluntarios). Esta función proporciona servicios seguros, de túnel, de Red privada virtual (VPN) multiprotocolo, sin que importe la topología de los suministradores de servicios. Esta función lleva al cliente y al LAC a una pieza física de hardware.
- Conexión de una llamada de entrada con la interfaz adecuada, basada en la coincidencia del nombre de sistema principal remoto. Si el nombre de sistema principal remoto no coincide con ninguna interfaz configurada para la coincidencia de nombres de sistema principal, se completa la llamada en una interfaz de entrada que no utiliza la coincidencia remota de nombres de sistema principal.

Nota: Si ha configurado varias correlaciones de red entre el mismo par de LAC y LNS, asegúrese de que existe un único túnel para cada correlación.

- La configuración automática de IP, IPX y de puente de las redes de entrada que no utiliza la coincidencia remota de nombres de sistema principal. Debe

Utilización de Layer 2 Tunneling

configurar manualmente las redes de salida y de entrada que utilizan la coincidencia remota de nombres de sistema principal.

Otros protocolos de Layer 2 Tunneling incluyen:

- Las funciones de L2F-Both NAS y de pasarela están soportadas.
- El cliente de Direccionador PPTP, PAC (Concentrador de acceso PPTP) y PNS (Servidor de red PPTP) están soportados.

L2F proporciona túneles interoperativos Layer 2 al conectar con dispositivos de red que no dan soporte a L2TP.

PPTP proporciona túneles interoperativos Layer 2 al conectar con dispositivos de red que no dan soporte a L2TP. PPTP puede utilizarse específicamente para los servicios VPN de Microsoft Windows 95 (DUN 1.2 y superior), Windows 98 y Windows NT a direccionadores IBM.

Nota: L2F y PPTP están configurados en la característica Layer 2 Tunneling.

Consideraciones sobre tiempo

La naturaleza de los túneles de paquetes PPP a través de las redes direccionadas, crea problemas de temporización que deben tenerse en cuenta. L2TP supone que la conexión entre el LAC y LNS no tiene un retardo que sea lo bastante prolongado para exceder el tiempo de espera de los similares con túneles. Si la latencia entre similares alcanza o sobrepasa de forma repetida el tiempo de espera de la máquina de estado PPP (por lo general, 3 segundos), la conectividad podría resultar perjudicada. Tenga en cuenta que, si la latencia entre el LAC y el LNS es tan baja, la conectividad en general también lo será, de manera que la conexión no será razonable, aunque se mantengan activas las máquinas de estado PPP de manera artificial. Si ambos lados poseen esta posibilidad, puede ampliarse el tiempo de espera de PPP para conseguir la conectividad a través de una conexión de muy baja calidad.

Además de la latencia, una falta de coincidencia del ancho de banda entre el par LAC/LNS y el par LAC/Cliente puede causar problemas. Si, por ejemplo, el ancho de banda real entre el LAC y el LNS es significativamente menor que el ancho de banda del cliente PPP, el LAC puede gastar un período de tiempo significativo intentando enviar paquetes al LNS. Por otra parte, si la conexión entre el LNS y un sistema principal en la red inicial de LNS es excepcionalmente rápida, comparada con el cliente de marcación de entrada, el LNS puede quedar sobrecargado mientras intenta enviar datos al LAC. L2TP implementa una serie de técnicas de control de flujo internos y externos en un intento de combatir estas situaciones.

Consideraciones sobre LCP

Al utilizar LCP de proxy, el LAC negocia el LCP y PPP continúa el proceso en el LNS. El LAC reenvía las opciones de LCP al LNS, de manera que el LNS conozca lo que se ha negociado. El LNS debe mantenerse flexible con los parámetros negociados por el cliente y el LAC. Si hay parámetros que son inaceptables para el LNS, L2TP intentará renegociar el LCP enviando una *Petición de configuración de LCP* al cliente a través del túnel.

El requisito del LNS para que permanezca flexible tiene una importancia particular respecto a la MRU. En el LNS de IBM, la MRU configurada es la máxima permitida para el LCP de proxy. Si el valor en el mensaje de LCP de proxy desde un LAC es mayor que la MRU configurada en el LNS, L2TP intentará renegociar el LCP con una MRU igual a la MRU configurada sin modificar otras opciones de LCP del LAC.

Configuración de Layer 2 Tunneling

Para configurar L2T:

1. Acceda a la característica Layer 2 Tunneling mediante el mandato **feature**.

```
Config> feature layer-2-tunneling
Layer-2-Tunneling config>
```

2. Habilite L2TP, L2F y PPTP de la manera adecuada.

```
Layer-2-Tunneling config> enable L2TP
Layer-2-Tunneling config> enable L2F
Layer-2-Tunneling config> enable pptp
```

3. Añada las redes L2T necesarias. Si va a ser estrictamente un LAC, NAS L2F o PAC PPTP, no es necesario que añada ninguna red L2T. Debe definir una red L2T para cada conexión PPP de túnel simultánea.

```
Layer-2-Tunneling Config>ADD L2-NETS
Additional L2 nets: [0]? 10
Add unnumbered IP addresses for each L2 net? [Yes]: yes
Adding device as interface 31
Defaulting Data-link protocol to PPP
Adding device as interface 32
Defaulting Data-link protocol to PPP
Adding device as interface 33
Defaulting Data-link protocol to PPP
Adding device as interface 34
Defaulting Data-link protocol to PPP
Adding device as interface 35
Defaulting Data-link protocol to PPP
Adding device as interface 36
Defaulting Data-link protocol to PPP
Adding device as interface 37
Defaulting Data-link protocol to PPP
Adding device as interface 38
Defaulting Data-link protocol to PPP
Adding device as interface 39
Defaulting Data-link protocol to PPP
Adding device as interface 40
Defaulting Data-link protocol to PPP
```

- a. Configure los túneles L2TP, L2F o PPTP.

Para configurar un túnel L2TP utilizando una lista local de AAA:

```
Config>add tunnel-profile
Enter name: []? lns.org
Tunneling Protocol? (PPTP, L2F, L2TP): L2TP
Enter local hostname: []? lac.org
set shared secret? (Yes, No): [No] Y
Shared secret for tunnel authentication:
Enter again to verify:
Tunnel-Server endpoint address: [0.0.0.0]? 11.0.0.1

PPP user name: lns.org
Tunnel Server: 11.0.0.1
Hostname: lac.org

User 'lns.org' has been added
Config>
```

Puede utilizar el ejemplo anterior para configurar la autorización de túnel en el LAC, así como los túneles “rhelm” con el formato “usuario@lns.org.”

Puede definir la autenticación y la autorización de túneles que debe realizarse en un servidor RADIUS determinado. Consulte “Using Authentication, Authorization, and Accounting (AAA) Security” en el manual *Utilización y configuración de las características*.

Si configura un LNS y la autenticación de túnel está inhabilitada en el LAC y el LNS, no es necesario configurar ningún perfil de túnel.

Para transportar por túnel según el nombre de usuario PPP en un LAC, utilizando una lista local de AAA o RADIUS:

```
Config>add ppp-user
Enter name: []? peter
Password:
Enter again to verify:
Allow inbound access for user? (Yes, No):[Yes]
Will 'peter' be tunneled? (Yes, No): [No] Y
Tunneling Protocol (PPTP, L2F, L2TP): [L2TP] L2TP
Enter local hostname: []? lac.org
Tunnel-Server endpoint address: [0.0.0.0]? 11.0.0.1

      PPP user name: peter
      Tunnel Server: 11.0.0.1
      Hostname: lac.org

Is information correct? (Yes, No, Quit): [Yes]

User 'peter' has been added
Config>
```

- b. Si es necesario, configure la coincidencia remota de nombres de sistema principal.

Tenga en cuenta que, para los escenarios de marcación de entrada del cliente, este paso no suele ser necesario. Utilice esta opción cuando una conexión debe especificar una red específica.

Suponiendo que la configuración anterior fuera para la red 10:

```
Config> net 10
L2TP 10> set remote-hostname
Remote Tunnel Hostname: [] ibm.com
```

Nota: Para desactivar la coincidencia remota de nombres de sistema principal, utilice los siguientes mandatos:

```
Config> net 10
L2TP 10> set any-remote-hostname
```

4. Configure cualquier llamada de salida L2TP. El siguiente ejemplo muestra un LAC con la dirección IP 1.1.1.1 y un LNS con la dirección IP 1.1.1.2. El LNS se configura para colocar una llamada RDSI de marcación bajo demanda a 5552160 desde el LAC.

Configuración de LNS:

```

Config> add tunnel-profile
Enter name: []? lac.org
Tunneling Protocol? (PPTP, L2F, L2TP): [L2TP]
Enter local hostname: []? lns.org
set shared secret? (Yes, No): [No] Y
Shared secret for tunnel authentication:
Enter again to verify:
Tunnel-Server endpoint address: [0.0.0.0]? 1.1.1.1

      Tunnel name: lac.org
      TunnType: L2TP
      Endpoint: 1.1.1.1
      Hostname: lns.org

User 'lac.org' has been added
Config>
Config> add dev layer-2-tunneling
Config> net 10
L2TP 10> set connection-direction outbound
L2TP 10> set idle 30
L2TP 10> set remote-hostname lac.org
L2TP 10> enable outbound-call-from-lac
      Outbound Call Type (ISDN)? [ISDN]
      Outbound calling address: 5552160
      Outbound calling subaddress:
L2TP 10>
L2TP 10> encapsulator
PPP 10> set name vickie a
L2TP 10>
L2TP 10> exit
Config> add ppp-user larry b

```

Notas:

- a. Defina el nombre de autenticación, en caso de que se realice la autenticación del dispositivo LNS. Hay indicadores adicionales que no aparecen en este ejemplo. Para más detalles, consulte “Configuring PPP Authentication” del capítulo “Using Point-to-Point Protocol Interfaces” del manual *Nways Multiprotocol Access Services Guía del usuario de software*.
- b. Añada usuarios que deben autenticarse en el LNS. Hay indicadores adicionales que no aparecen en este ejemplo. Consulte Add en el capítulo “The CONFIG Process (CONFIG - Talk 6) and Commands” del manual *Nways Multiprotocol Access Services Guía del usuario de software* para ver una descripción de la sintaxis del mandato y sus opciones.

Configuración de LAC:

```

Config> add tunnel-profile
Enter name: []? lns.org
Tunneling Protocol? (PPTP, L2F, L2TP): [L2TP]
Enter local hostname: []? lac.org
set shared secret? (Yes, No): [No] Y
Shared secret for tunnel authentication:
Enter again to verify:
Tunnel-Server endpoint address: [0.0.0.0]? 1.1.1.2

      Tunnel name: lns.org
      TunnType: L2TP
      Endpoint: 1.1.1.1
      Hostname: lac.org

User 'lns.org' has been added
Config>
Config> add dev dial-in a

```

Notas:

- a. Se utiliza para hacer la llamada física.
5. Configure cualquier cliente de direccionador L2T. El siguiente ejemplo muestra una conexión de cuadro a cuadro L2TP utilizando la función del cliente de direccionador L2TP. Esta conexión se define en una dirección y está basada en la demanda.

Configuración de cliente:

```
Config> add tunnel-profile
Enter name: []? lns.org
Tunnel Protocol? (PPTP, L2T, L2TP): [L2TP]
Enter local hostname: []? client.org
set shared secret? (Yes, No): [No] Y
Shared secret for tunnel authentication:
Enter again to verify:
Tunnel-Server endpoint address: [0.0.0.0]? 1.1.1.1

Tunnel name: lns.org
TunnType: L2TP
Endpoint: 1.1.1.1
Hostname: client.org

User 'lns.org' has been added
Config>
Config> add dev layer-2-tunneling
Config> net 10
L2TP 10> set connection-direction outbound
L2TP 10> set idle 30
L2TP 10> set remote-hostname lns.org
L2TP 10> encapsulator
PPP 10> set name donald a
PPP 10> exit
L2TP 10> exit
Config>
```

Nota: **a** — Defina el nombre de autenticación, en caso de que realice la autenticación del dispositivo de cliente. Hay indicadores adicionales que no aparecen en este ejemplo. Para más detalles, consulte “Configuring PPP Authentication” del manual *Nways Multiprotocol Access Services Guía del usuario de software*.

Configuración de LNS:

```

Config> add tunnel-profile
Enter name: []? client.org
Tunneling Protocol? (PPTP, L2F, L2TP): [L2TP]
Enter local hostname: []? lns.org
set shared secret? (Yes, No): [No] Y
Shared secret for tunnel authentication:
Enter again to verify:
Tunnel-Server endpoint address: [0.0.0.0]? 1.1.1.2

Tunnel name: client.org
TunnType: L2TP
Endpoint: 1.1.1.2
Hostname: lns.org

User 'client.org' has been added
Config>
Config> add dev layer-2-tunneling
Config> net 10
L2TP 10> set connection-direction inbound
L2TP 10> set remote-hostname client.org
L2TP 10> encapsulator
Config>
Config> add ppp-user donald b
Config>

```

Nota: b— Añada usuarios que deben autenticarse en el LNS. Hay indicadores adicionales que no aparecen en este ejemplo. Para obtener más detalles, consulte “**add Config command**” en el manual *Nways Multiprotocol Access Services Guía del usuario de software*.

- Si lo desea, configure los diversos parámetros de L2T de característica, mediante los mandatos **set** y **enable**.

```

Layer-2-Tunneling Config>set ?
Layer-2-Tunneling Config>enable ?

```

- Configure los parámetros de PPP para todas las redes L2 que están definidas para el nombre, *cualquiera*, de sistema principal de túnel de entrada, utilizando el mandato de encapsulador.

```

Layer-2-Tunneling Config>encapsulator
PPP-L2TP Config>

```

Cuando haya completado la configuración de PPP, entre **exit** para regresar al entorno de configuración de característica L2T.

Configuración y supervisión de protocolos Layer 2 Tunneling

Este capítulo describe los mandatos operativos y de configuración de Layer 2 tunneling (L2T). L2T incluye los protocolos L2TP (Layer 2 Tunneling Protocol), L2F (Layer 2 Forwarding Protocol) y PPTP (Point-to-Point Tunneling Protocol). Las secciones de este capítulo son:

- “Acceso al indicador de configuración de la interfaz L2T”
- “Mandatos de configuración de la interfaz L2 Tunneling”
- “Acceso al indicador de configuración de la característica L2 Tunneling” en la página 455
- “Mandatos de configuración de la característica L2 Tunneling” en la página 455
- “Acceso al indicador de supervisión de L2 Tunneling” en la página 460
- “Mandatos de supervisión de L2 Tunneling” en la página 461

Acceso al indicador de configuración de la interfaz L2T

Para acceder al indicador de configuración de la interfaz L2T:

1. Entre **talk 6** en el indicador OPCON (*).
2. Entre **add dev layer-2-tunneling** en el indicador Config> (o utilice el mandato **add l2-nets**. Consulte “Add” en la página 456).
3. Entre **n número-interfaz** en el indicador Config>.

```
Config> add device layer-2-tunneling
Enter the number of Layer-2-Tunneling interfaces [1]
Adding device as interface 8
Defaulting Data-link protocol to PPP
Config> n 8
Session configuration
L2T config: 8>
```

Mandatos de configuración de la interfaz L2 Tunneling

La Tabla 55 resume los mandatos de configuración de la interfaz L2T. Entre estos mandatos en el indicador L2T Config n> (donde n es el número de red).

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxiv.
Disable	Inhabilita las llamadas de salida.
Enable	Habilita las llamadas de salida.
Encapsulator	Permite configurar los parámetros de PPP en la interfaz L2T. Nota: La opción de encapsulador sólo está disponible si una interfaz tiene configurado un nombre de sistema principal remoto.
List	Visualiza información acerca de la interfaz L2T.
Set	Permite definir varios parámetros de interfaz L2T.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiv.

Mandatos de configuración de la interfaz L2 Tunneling (Talk 6)

Disable

Utilice el mandato **disable** para inhabilitar llamadas de salida desde el concentrador de acceso L2TP (LAC).

Sintaxis: `disable` `outbound-calls-from-lac`

outbound-calls-from-lac

Evita que el LNS inicie una señal de marcación desde el LAC a través de un túnel L2TP.

Enable

Utilice el mandato **enable** para habilitar llamadas de salida desde el concentrador de acceso L2TP (LAC). Este mandato debe utilizarse sólo con L2TP.

Sintaxis:

`enable` `outbound-calls-from-lac`

outbound-calls-from-lac

Permite que el LNS inicie una señal de marcación desde el LAC a través de un túnel L2TP.

Ejemplo:

```
L2T 10> enable outbound-call-from-lac
Outbound Call Type (ISDN)? [ISDN]
Outbound calling address: 1234
Outbound calling subaddress:
L2T 10>
```

Encapsulator

Utilice el mandato **encapsulator** para configurar los parámetros de PPP para la interfaz L2T.

Sintaxis: `encapsulator`

Este mandato sólo está disponible cuando se ha configurado un nombre de sistema principal remoto. Para obtener una lista de mandatos disponibles en el indicador `ppp-L2tp config>`, consulte "Encapsulator" en la página 458.

List

Utilice el mandato **list** para visualizar el estado de los parámetros de configuración de interfaz L2T.

Sintaxis: `list`

```
Layer-2-Tunneling Config>list
CONNECTION TYPE
-----
Connection Direction          INBOUND
Remote Tunnel Hostname        *ANY*
```

Set

Utilice el mandato **set** para configurar los parámetros operativos de la interfaz L2T.

Sintaxis: `set` `any-remote-hostname`
`connection-direction`
`idle`
`remote-hostname`

Mandatos de configuración de la característica L2 Tunneling (Talk 6)

any-remote-hostname

Borra el nombre de sistema principal remoto de salida e inhabilita el nombre de sistema principal remoto de entrada coincidente en esta red.

connection-direction [inbound] o [outbound] o [both]

Especifica si la entidad similar (inbound), el dispositivo local (outbound), o ambos (both) en esta red pueden iniciar la conexión. Si especifica ambos (both), no puede especificar un valor cero para el tiempo de desocupado.

Valor por omisión: inbound

idle-time segundos

Especifica el número de segundos de inactividad, después de los cuales el túnel L2 desconectará la sesión de túnel en esta red. El valor cero indica que el túnel es fijo y no se debe desconectar.

Valores válidos: 0 a 1024

Valor por omisión: 0

remote-hostname nombre-sistema-principal

Especifica el nombre de sistema principal de túnel para la entidad similar.

Para un túnel de salida, el nombre de sistema principal especifica un perfil de túnel configurado en el subsistema AAA. Debe ser el nombre de sistema principal de túnel que utiliza el similar para identificarse.

Para un túnel de entrada, sólo los similares de túnel que se identifiquen con este nombre de sistema principal pueden conectarse a esta interfaz.

Valores válidos: cualquier nombre de 1 a 64 caracteres ASCII

Valor por omisión: *Nombre*

Acceso al indicador de configuración de la característica L2 Tunneling

Para acceder al indicador de configuración de la característica L2 Tunneling:

1. Entre **talk 6** en el indicador OPCON (*).
2. Entre **feature layer-2-tunneling** en el indicador Config>.

Mandatos de configuración de la característica L2 Tunneling

La Tabla 56 en la página 456 resume los mandatos de configuración de la característica L2 Tunneling y el resto de esta sección explica los mandatos. Entre estos mandatos en el indicador Layer-2-Tunneling Config>.

Mandatos de configuración de la característica L2 Tunneling (Talk 6)

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxiv.
Add	Añade redes y similares de L2 Tunneling.
Disable	Inhabilita las funciones de L2 Tunneling.
Enable	Habilita las funciones de L2 Tunneling.
Encapsulator	Permite configurar parámetros de PPP para todas las redes de L2 Tunneling que no están configuradas con un nombre de sistema principal remoto (ANY).
List	Visualiza información acerca de la configuración de L2 Tunneling.
Set	Permite definir almacenamientos intermedios, la ventana de recepción de llamadas y otros parámetros de L2 Tunneling.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiv.

Add

Utilice el mandato **add** para añadir L2-Nets. Se requiere una L2-Net por cada sesión PPP simultánea que finalice en este direccionador. El fin de una sesión PPP de túnel es el extremo LNS del túnel.

Sintaxis: `add L2-nets`

L2-nets

Nota: Este mandato se puede entrar por completo en minúsculas. El carácter inicial se muestra en mayúsculas para una mayor claridad.

Añade L2-Nets a la configuración de túnel L2. Se requiere una L2-Net por cada sesión PPP simultánea que debe terminar en este direccionador. Si este direccionador va a utilizarse estrictamente como LAC, no se necesita ninguna L2-Net virtual. Al entrar este mandato, se le solicitará el número de redes adicionales y si se deben añadir direcciones IP sin número para cada red L2.

El número de redes adicionales hace referencia a cuántas redes se añaden automáticamente en estos momentos. Estas redes deben añadirse a las L2-Nets que ya existan.

La adición de direcciones IP no numeradas para cada L2-Net añade automáticamente entradas IP no numeradas a la tabla de direccionamiento de IP para cada una de las L2-Nets. Las direcciones IP no numeradas son la modalidad favorita de operación. Si necesita direcciones numeradas para las L2-Nets, puede alterarlas en el entorno de configuración de protocolo IP (consulte el capítulo titulado “Configuring IP” del manual *Consulta de configuración y supervisión de protocolos Volumen 1*).

Disable

Utilice el mandato **disable** para inhabilitar las funciones de túnel de L2.

Sintaxis: `disable` `call-rcv-window`
`fixed-udp-source-port`
`force-chap-challenge`
`hiding-for-pap-attributes`
`L2f`
`L2tp`

Mandatos de configuración de la característica L2 Tunneling (Talk 6)

pptp
proxy-~~a~~uth
proxy-lcp
tunnel-~~a~~uth

call-rcv-window

Los túneles L2 pueden poner paquetes en cola para cada llamada con el fin de realizar el control de puesta en secuencia y de congestión. Cada llamada tiene su propia ventana, que es el número de paquetes que pueden enviarse antes de recibir un ACK. La inhabilitación de *call-rcv-window* desactiva el control de flujo y la puesta en secuencia para toda la sesión. Esto puede ser deseable cuando se sabe que la conexión entre el LAC y el LNS es de alta calidad, con un ancho de banda suficiente y muy poco proclive a la reordenación de paquetes.

fixed-udp-source-port

Borra utilizando un puerto UDP fijo. La inhabilitación de este parámetro obliga a que la dirección IP configure filtros de Seguridad de IP entre el LAC y el LNS.

force-chap-challenge

Inhabilita el redesafío LNS CHAP de un cliente. Puede que tenga que inhabilitar el redesafío CHAP si el cliente PPP tiene dificultades con los redesafíos CHAP.

hiding-for-pap-attributes

Inhabilita el cifrado de la información de PAP Proxy entre el LAC y el LNS.

L2f Inhabilita el protocolo L2F en este direccionador.

L2tp

Inhabilita el protocolo L2TP en este direccionador.

pptp

Inhabilita el protocolo PPTP en este direccionador.

proxy-auth

Inhabilita el envío de la autenticación de proxy PPP desde LAC a LNS.

proxy-lcp

Inhabilita el envío de información de LCP desde LAC a LNS.

tunnel-auth

Inhabilita la autenticación de similar de túnel, basada en un secreto compartido para este direccionador.

Enable

Utilice el mandato **enable** para habilitar las funciones de túnel de L2.

Sintaxis:

enable fixed-udp-source-port
 force-chap-challenge
 hiding-for-pap-attributes
 L2f
 L2tp
 pptp
 proxy-~~a~~uth
 proxy-lcp

Mandatos de configuración de la característica L2 Tunneling (Talk 6)

`tunnel-auth`

fixed-udp-source-port

La habilitación de este parámetro le permite configurar filtros de Seguridad de IP por puerto UDP para túneles L2, de manera que puede cifrar o autenticar fácilmente el tráfico de túneles L2. Defina el puerto UDP como 1701 para L2TP.

force-chap-challenge

Habilita el redesafo LNS CHAP de un cliente, aunque el LNS reciba un CHAP proxy. Esto es preferible desde el punto de vista de la seguridad, si se sabe que el cliente puede gestionar semejante redesafo sin problemas.

hiding-for-pap-attributes

Habilita el cifrado de la información de PAP Proxy entre el LAC y el LNS.

L2f Habilita el protocolo L2F en este direccionador.

L2tp

Habilita el protocolo L2TP en este direccionador.

pptp

Habilita el protocolo PPTP en este direccionador.

proxy-auth

Habilita el envío de la autenticación de proxy PPP desde LAC a LNS.

proxy-lcp

Habilita el envío de información de LCP desde LAC a LNS.

tunnel-auth

Habilita la autenticación de similar de túnel, basada en un secreto compartido para este direccionador.

Encapsulator

Utilice el mandato **encapsulator** para acceder al indicador `ppp-L2tp config>`, con el fin de configurar los parámetros PPP para todas las interfaces de Layer 2 Tunneling configuradas como de entrada y *cualquier* nombre de sistema principal remoto.

Sintaxis: `encapsulator`

List

Utilice el mandato **list** para visualizar el estado de los diversos parámetros de configuración de túnel de L2.

Sintaxis: `list`

Mandatos de configuración de la característica L2 Tunneling (Talk 6)

```
Layer-2-Tunneling Config>list
GENERAL ADMINISTRATION
-----
L2TP                               = Enabled
L2F                                 = Disabled
PPTP                                = Disabled
Maximum number of tunnels           = 20
Maximum number of calls (total)     = 50
Buffers Requested                   = 300

CONTROL CHANNEL SETTINGS
-----
Tunnel Auth                         = Enabled
Tunnel Rcv Window                   = 4
Retransmit Retries                  = 6
Local Hostname                      = Host6

DATA CHANNEL SETTINGS
-----
Force CHAP Challenge (extra security)= Disabled
Hiding for PAP Attributes            = Disabled
Hardware Error Polling Period (Sec) = 120
Call Rcv Window                     = 6

MISCELLANEOUS
-----
SEND PROXY-LCP FROM LAC             = Enabled
SEND PROXY-AUTH FROM LAC            = Enabled
Fixed UDP Source Port (1701)        = Disabled
```

Set

Utilice el mandato set para configurar los parámetros operativos de L2 Tunneling.

Sintaxis: set buffers
call-rcv-window
error-check-direction
host-lookup-password
local-hostname
max-calls
max-tunnels
transmit-retries
tunnel-rcv-window

buffers

Especifica el número de almacenamientos intermedios internos de L2 Tunneling solicitados. Si no hay memoria suficiente para satisfacer esta petición, sólo una parte de los almacenamientos intermedios estará disponible al rearrancar. Para confirmar la cantidad de memoria mientras L2T está activo, utilice el mandato **memory** (consulte “Memory” en la página 464).

Valores válidos: 1 a 1000

Valor por omisión: 200

call-rcv-window

Especifica el número de paquetes que deben utilizarse como ventana de recepción y habilita call-rcv-window. Si el control de flujo está habilitado en el canal de datos, es preciso designar el tamaño de la ventana de recepción, tanto para su uso por el protocolo en este direccionador, como para la comunicación con la entidad similar utilizando mensajes de arranque. El valor configurado es para todas las llamadas iniciadas por este direccionador. El valor cero significa que sólo es secuencia (sin control de flujo).

Valores válidos: 0 a 100

Valor por omisión: 0

error-check-period [seconds]

Especifica el período de sondeo de errores de hardware del LAC. Cada período de sondeo dará como resultado un mensaje WAN Error Notify, transmitido desde el LAC al LNS. El rango abarca de 60 a 65000 segundos.

Valor por omisión: 120 segundos.

host-lookup-password

Especifica el secreto compartido para la autorización de túnel RADIUS. Debe coincidir con el secreto configurado en el servidor.

Valor por omisión: ninguno.

local-hostname

Especifica la serie de nombre de sistema principal que identifica el direccionador local que se envía en los mensajes de configuración de túnel.

Valor por omisión: IBM

max-calls

Especifica el número máximo de llamadas entre todos los túneles que pueden estar activos en un momento determinado, como LAC o LNS.

Valores válidos: 1 a 500

Valor por omisión: 100

max-tunnels

Especifica el número máximo de túneles que pueden estar activos en un momento determinado, como LAC o LNS.

Valores válidos: 1 a 100

Valor por omisión: 30

transmit-retries

Especifica el número de veces que un paquete L2TP se retransmite en el canal de control antes de que la sesión o el túnel sea declarado inactivo y se concluya.

Valores válidos: 2 a 100

Valor por omisión: 6

tunnel-rcv-window

Especifica el tamaño de la ventana de recepción de L2TP para el transporte de conexiones de control de confianza. Este transporte transmite y recibe los mensajes necesarios para la configuración de túnel o de sesión, división y mantenimiento.

Valores válidos: 1 a 100

Valor por omisión: 4

Acceso al indicador de supervisión de L2 Tunneling

Para acceder al indicador de supervisión de L2 Tunneling:

1. Entre **talk 5** en el indicador OPCON (*).
2. Entre **feature layer-2-tunneling** en el indicador GWCON (+).

Mandatos de supervisión de L2 Tunneling

Esta sección resume y describe los mandatos de supervisión de L2 Tunneling. Entre los mandatos en el indicador Layer-2-Tunneling Console>.

La Tabla 57 resume los mandatos de supervisión de L2 Tunneling.

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado "Cómo obtener ayuda" en la página xxxiv.
Call	Visualiza estadísticas e información acerca de cada llamada en proceso.
Kill	Finaliza un túnel de inmediato.
Memory	Visualiza la asignación y la utilización actuales del almacenamiento intermedio de L2 Tunneling.
Start	Inicia un túnel con otro similar.
Stop	Detiene un túnel y permite que cada similar realice cualquier operación de administración necesaria.
Tunnel	Visualiza estadísticas e información sobre cada túnel existente.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página xxxiv.

Call

Utilice el mandato **call** para visualizar estadísticas e información sobre llamadas.

Sintaxis: `call errors`
`physical-errors`
`queue`
`state`
`statistics`

errors

Visualiza los errores generales de transmisión que se han producido en las llamadas.

Ejemplo:

```
Layer-2-Tunneling Console> call errors
CallID | Serial # | ACK-timeout | Dropped pkts
56744 | 1 | 0 | 0
```

CallID

Identificador local asociado con esta llamada.

Serial

Número utilizado para registrar cronológicamente esta llamada.

ACK-timeout

Número de veces que se ha recibido del similar una notificación de tiempo de espera excedido.

Dropped pkts

Número de paquetes que se han declarado perdidos para esta llamada. Son paquetes que se deberían haber recibido, pero el similar los ha señalado como perdidos.

Mandatos de supervisión de L2 Tunneling (Talk 5)

physical-errors

Visualiza los errores de datos que se han producido en las llamadas.

Ejemplo:

```
Layer-2-Tunneling Console> call physical-errors
CallID | Serial# | CRC | framing | HW | buffer | timeout | align- | time since
Errors | Errors | overrun | overrun | Errors | ment | updated
56744 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0
```

CallID

Identificador local asociado con esta llamada.

Serial

Número utilizado para registrar cronológicamente esta llamada.

CRC Errors

Número de paquetes en que el CRC no coincide.

framing errors

Número de paquetes con error de trama.

HW overrun

Número de veces que se ha producido un desbordamiento de hardware.

buffer overrun

Número de veces que se ha producido un desbordamiento de almacenamiento intermedio.

timeout errors

Número de veces que se ha excedido el tiempo de espera de una interfaz.

alignment

Número de veces que se ha producido un error de alineación.

time since updated

Tiempo transcurrido desde el último sondeo para errores.

queue

Visualiza información acerca de la cola para cada llamada.

Ejemplo:

```
Layer-2-Tunneling Console> call queue
CallID | Serial # | Tx Win | Rx Win | Ns | Nr | Rx Q | Tx Q | priority | out Q
56744 | 1 | 4 | 4 | 100 | 200 | 0 | 0 | 0 | 0
```

CallID

Identificador local asociado con esta llamada.

Serial

Número utilizado para registrar cronológicamente esta llamada.

Tx Win

Ventana máxima de recepción del similar para datos.

Rx Win

Ventana máxima de transmisión local.

Ns Siguiete número de secuencia de paquetes que se envía para esta llamada.

Nr Siguiete número de secuencia de paquetes que se espera recibir para esta llamada.

Rx Q

Número actual de paquetes en la cola de recepción.

Tx Q

Número actual de paquetes en la cola de transmisión.

priority

Número de paquetes PPP de prioridad que esperan a ser transmitidos por L2TP.

out Q

Número de paquetes PPP regulares que esperan a ser transmitidos por L2TP.

state

Visualiza el estado actual de cada llamada.

Ejemplo:

```
Layer-2-Tunneling Console> call state
CallID | Serial # | Net # | State | Time Since Chg | PeerID | TunnelID
56744 | 1 | 2 | Established | 00:00:00 | 345 | 45678
```

CallID

Identificador local asociado con esta llamada.

Serial

Número utilizado para registrar cronológicamente esta llamada.

Net

Número de dispositivo asociado con esta llamada. Para una llamada de LNS, es la L2-Net. Para una llamada de LAC, es el dispositivo PPP que ha recibido la llamada inicial.

State

Estado de llamada actual. Los estados de llamada válidos son:

Established

Listo para el tráfico de red por túnel.

Idle

La llamada está desocupada.

Wait Cs Answer

Espera a que se abra el enlace de comunicación.

Wait Reply

Espera una respuesta del similar.

Wait Tunnel

Espera el restablecimiento de túnel.

Time since chg

Tiempo transcurrido desde el último cambio de estado.

PeerID

ID de llamada del similar.

TunnelID

Túnel local asociado con esta llamada.

statistics

Visualiza estadísticas acerca de la transmisión de datos para cada llamada.

Mandatos de supervisión de L2 Tunneling (Talk 5)

Ejemplo:

```
Layer-2-Tunneling Console> call statistics
CallID | Serial # | Tx Pkts | Tx Bytes | Rx Pkts | Rx Bytes | RTT | ATO
56744 | 1 | 34 | 1056 | 45 | 1567 | 10 | 34
```

CallID

Identificador local asociado con esta llamada.

Serial

Número utilizado para registrar cronológicamente esta llamada.

Tx Pkts

Número de paquetes transmitidos para esta llamada.

Tx Bytes

Número de bytes transmitidos para esta llamada.

Rx Pkts

Número de paquetes recibidos para esta llamada.

Rx Bytes

Número de bytes recibidos para esta llamada.

RTT

Tiempo de ida y vuelta calculado actualmente para esta llamada.

ATO

Tiempo de espera de adaptación calculado actualmente para esta llamada.

Kill

Utilice el mandato **kill** para finalizar un túnel de inmediato. Este mandato libera todos los recursos locales para un túnel, forzando así el fin de la conexión. No se envía al similar ninguna notificación del fin del túnel.

Nota: Utilice sólo este mandato si el mandato **stop** no puede finalizar un túnel.

Sintaxis: `kill tunnel id-túnel`

tunnel id-túnel

Especifica que finalice el túnel.

Memory

Utilice el mandato **memory** para visualizar la utilización actual de memoria de L2TP.

Sintaxis: `memory`

Ejemplo:

```
Layer-2-Tunneling Console> mem
Number of layer-2-tunneling buffers: Requested = 2000, Total = 1200, Free
= 1000
```

En este ejemplo, ha configurado 2000 almacenamientos intermedios, pero sólo ha podido asignar 1200. Actualmente, se están utilizando 200 almacenamientos intermedios, dejando 1000 libres.

Start

Utilice el mandato **start** para iniciar un túnel con otro similar.

Sintaxis: `start` (ningún parámetro solicita el nombre de sistema principal)
`tunnel hostname`

hostname

Nombre del sistema principal con el que L2T establece el túnel.

Stop

Utilice el mandato **stop** para detener un túnel. Antes de que finalice el túnel, se completa cualquier borrado necesario.

Sintaxis: `stop tunnel id-túnel`

tunnel id-túnel

Especifica que finalice el túnel.

Tunnel

Utilice el mandato **tunnel** para visualizar estadísticas e información acerca de todos los túneles.

Sintaxis: `tunnel call`

`errors`

`peer`

`queue`

`state`

`statistics`

`transport`

calls

Visualiza todos los túneles y el estado de llamada para cada llamada en cada túnel.

errors

Visualiza los errores producidos en un túnel.

Ejemplo:

```
Layer-2-Tunneling Console> tunnel errors
Tunnel ID | Type | ACK-timeouts
96785     | L2TP | 0
43690     | PPTP | 2
96785     | L2F  | 0
```

Tunnel ID

Identificador local asociado con un túnel.

Type

Tipo de protocolo de túnel que se utiliza.

ACK-timeouts

Número de veces que se ha recibido del similar una notificación de tiempo de espera excedido.

peer

Visualiza los túneles y los similares asociados a los túneles.

Mandatos de supervisión de L2 Tunneling (Talk 5)

Ejemplo:

```
Layer-2-Tunneling Console> tunnel peer
Tunnel ID | Type | Peer ID | Peer Hostname
96785     | L2TP | 89777   | peer1
11264     | L2F  | 46538   | peer2
34653     | L2F  | 11209   | peer3
87511     | PPTP | 55377   | peer4
```

Tunnel ID

Identificador local asociado con un túnel.

Type

Tipo de protocolo de túnel que se utiliza.

Peer ID

Identificador de túnel del similar que se ha asignado a este túnel.

Peer Hostname

Nombre de sistema principal del similar tal como aparece en la base de datos local.

queue

Visualiza información acerca de la cola para cada túnel.

Ejemplo:

```
Layer-2-Tunneling Console> tunnel queue
Tunnel ID | Type | Rx Win | Tx Win | Ns | Nr | Rx Q | Tx Q
96785     | L2TP | 4       | 4       | 5  | 6  | 0     | 0
76488     | L2F  | 4       | 4       | 5  | 6  | 0     | 0
22209     | PPTP | 4       | 4       | 5  | 6  | 0     | 0
```

Tunnel ID

Identificador local asociado con un túnel.

Type

Tipo de protocolo de túnel que se utiliza.

Rx Win

Número máximo local de paquetes que constituyen la ventana de recepción.

Tx Win

Número máximo de paquetes del similar que constituyen la ventana de recepción.

Ns Número de secuencia del siguiente paquete que se envía.

Nr Número de secuencia del siguiente paquete que se recibe.

Rx Q

Número actual de paquetes en la cola de recepción.

Tx Q

Número actual de paquetes en la cola de transmisión.

state

Visualiza el estado actual de todos los túneles.

Ejemplo:

```
Layer-2-Tunneling Console> tunnel state
Tunnel ID | Type | Peer ID | State | Time Since Chg | # Calls | Flags
17404     | PPTP | 0       | Established | 00:00:00 | 1 | 0
96785     | L2TP | 0       | Established | 00:02:05 | 2 | 0
38237     | L2F  | 0       | Established | 00:00:00 | 1 | 0
```

Tunnel ID

Identificador local asociado con un túnel.

Type

Tipo de protocolo de túnel que se utiliza.

Peer ID

Identificador de túnel del similar que se ha asignado a este túnel.

State

Estado actual del túnel. Los estados de túnel válidos son:

Established

El túnel está establecido.

Idle

El túnel está desocupado.

Wait Ctrl Reply

El sistema principal espera una respuesta del similar.

Wait Ctrl Conn

El sistema principal espera una indicación de conexión.

Time since chg

Tiempo transcurrido desde el último cambio de estado.

Calls

Número de llamadas activas en este túnel.

Flags

Distintivos utilizados para controlar los mensajes de conexión en este túnel.

statistics

Visualiza las estadísticas asociadas con los túneles.

Ejemplo:

```
Layer-2-Tunneling Console> tunnel statistics
Tunnel ID | Type | Tx Pkts | Tx Bytes | Rx Pkts | Rx Bytes | RTT | ATO
96785    | L2TP | 4       | 78       | 5       | 89       | 10  | 31
96366    | L2F  | 9344   | 34578   | 305     | 4300     | 10  | 31
12344    | PPTP | 24     | 478     | 115     | 2745     | 10  | 31
```

Tunnel ID

Identificador local asociado con un túnel.

Type

Tipo de protocolo de túnel que se utiliza.

Tx Pkts

Número de paquetes transmitidos.

Tx Bytes

Número de bytes transmitidos.

Rx Pkts

Número de paquetes recibidos.

Rx Bytes

Número de bytes recibidos.

RTT

Tiempo de ida y vuelta calculado actualmente para los mensajes de conexión de control de túnel.

Mandatos de supervisión de L2 Tunneling (Talk 5)

ATO

Tiempo de espera de adaptación calculado actualmente para los mensajes de conexión de control de túnel.

transport

Visualiza información de UDP acerca de los túneles.

Ejemplo:

```
Layer-2-Tunneling Console> tunnel transport
Tunnel ID | Type | Peer IP Address | UDP Src | UDP Dest
96785     | L2TP | 11.0.0.102      | 1056    | 1089
30000     | L2F  | 11.0.0.104      | 1058    | 1090
45772     | PPTP | 11.4.4.027      | 1345    | 1020
```

Tunnel ID

Identificador local asociado con un túnel.

Type

Tipo de protocolo de túnel que se utiliza.

Peer IP address

Dirección IP del similar para este túnel.

UDP Src

Puerto UDP de origen para este túnel.

UDP Dest

Puerto UDP de destino para este túnel.

Utilización de la conversión de direcciones de red

La Conversión de direcciones de red (NAT) y su extensión Conversión de direcciones de red y puertos (NAPT) pueden ampliar el número de las direcciones IP disponibles para una organización y puede evitar a los usuarios de la red pública que conozcan algunas de las direcciones de la red privada. NAT funciona utilizando direcciones IP públicas para representar direcciones IP privadas.

Las direcciones IP públicas son las direcciones válidas de los sistemas principales en la red IP pública y deben ser exclusivas en la red pública. Si la red pública es Internet, las direcciones IP públicas deben ser direcciones Internet exclusivas, proporcionadas por el Network Information Center (NIC).

Las direcciones privadas son conocidas para el direccionador, pero no para la red pública. Las direcciones en cada red privada deben ser exclusivas; no obstante, puede duplicarse la misma dirección en dos redes privadas distintas. Las direcciones privadas se asignan a los sistemas principales en redes de apéndice. Las redes de apéndice son redes que tienen acceso a la red pública a través de un único direccionador.

NAT amplía de varias maneras el número de direcciones IP disponibles:

- Permite que cada dirección pública represente varias direcciones privadas rotando el uso de las direcciones públicas.
- Permite la duplicación de direcciones, mientras se utilice cada dirección duplicada en una red privada distinta.
- Permite al administrador de red utilizar direcciones IP en las redes privadas, en lugar de las direcciones NIC, que se están convirtiendo en recursos limitados.

La utilización de direcciones privadas también oculta estas direcciones del mundo exterior. Esta característica de NAT hace que resulte útil como un tipo de cortafuegos para proteger las direcciones privadas de que lleguen a ser conocidas.

Importante: Como se indica en la sección 5.4 del Internet Draft que define NAT, “cualquier aplicación que transporte (y utilice) la dirección IP (y el puerto TCP/UDP, en el caso de NAPT) en el interior de la aplicación no pasará por NAT...”. Debe tenerse en cuenta que DLSw y XTP toman decisiones basadas en las direcciones IP de extremo y, específicamente, qué asociado tiene la dirección más elevada. Dado que la aplicación (como DLSw o XTP) que se ejecuta a través de NAT considera que su dirección es la dirección privada, mientras que la aplicación asociada que se encuentra en el otro direccionador considera que la dirección de la aplicación es la dirección pública, pueden tomarse decisiones incorrectas.

Vea un plano de una estación de trabajo en una red de apéndice en la Figura 41 en la página 470. En este ejemplo, la red de apéndice consiste en una subred IP que tiene la dirección IP 10.33.96.0 con la máscara de subred 255.255.255.0.

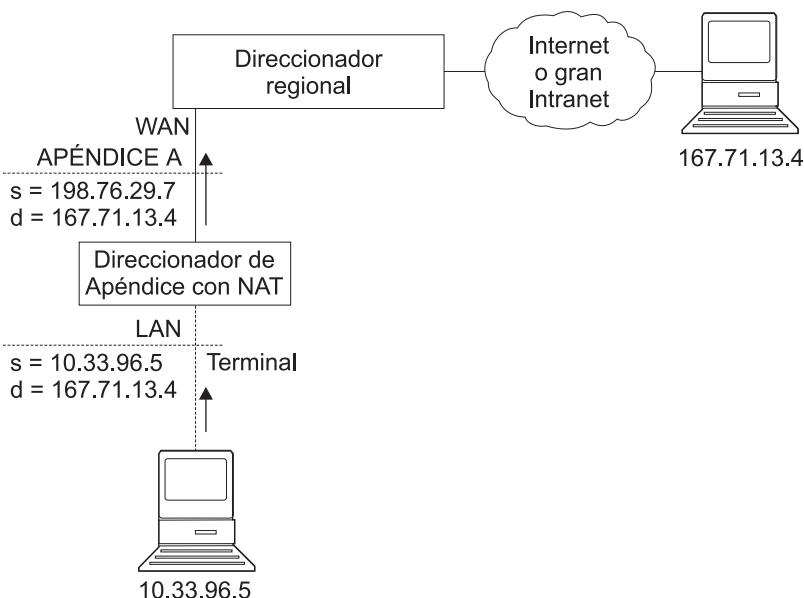


Figura 41. Red que ejecuta NAT

Para utilizar NAT, el administrador de red asigna una o más direcciones IP públicas a una agrupación de direcciones públicas en el 2216 y asigna una dirección IP privada a cada estación de trabajo de la red de apéndice. Las direcciones IP públicas se asignan a una *agrupación de reserva* y las direcciones IP privadas se asignan al *rango de conversión*.

En primer lugar, la función NAT vincula la dirección privada de una estación de la red privada con una de las direcciones públicas. Este vínculo significa que todos los paquetes que tengan esa dirección privada se convertirán a esa dirección IP pública cuando salgan. Los paquetes de entrada tienen la dirección IP pública como destino. NAT reconoce la dirección pública, la convierte a la dirección IP privada y reenvía el paquete. Después de la detención del tráfico, el vínculo se mantiene hasta que se exceda el tiempo de espera definido por el usuario en un temporizador. En ese momento, NAT finaliza el vínculo y pone la dirección pública a disposición para que vuelva a utilizarse.

En este ejemplo se transmite un paquete, enviándolo desde la dirección origen privada 10.33.96.5 a la dirección de destino en Internet 167.71.13.4. En el 2216, NAT convierte la dirección privada 10.33.96.5 en la dirección pública 198.76.29.7. Esta conversión oculta la dirección privada 10.33.96.5 de la red pública, de manera que ningún paquete entrante se dirige directamente a la dirección privada 10.33.96.5. Los paquetes entrantes de 167.71.13.4 se dirigen a la dirección pública 198.76.29.7. Cuando el direccionador de NAT recibe paquetes dirigidos a 198.76.29.7, NAT convierte la dirección pública de destino a la dirección privada 10.33.96.5 y reenvía los paquetes.

Conversión de puertos de direcciones de red

NAPT sólo puede utilizarse para el tráfico de TCP y UDP. En NAPT, varias direcciones privadas pueden utilizar simultáneamente una sola dirección pública. Mientras NAT correlaciona una dirección pública con una dirección privada, NAPT correlaciona la dirección pública de NAPT y el número de puerto público con una

dirección privada y un número de puerto privado. Sólo puede configurarse una dirección de NAPT para cada agrupación de direcciones públicas.

Para configurar NAPT, basta con especificar una dirección pública o una interfaz de Dirección dinámica (que utiliza PPP/IPCP para recuperar una dirección pública) que se utilizará para el tráfico de NAPT. La ventaja de NAPT es que puede habilitar una dirección de la agrupación de direcciones IP públicas para dar soporte a muchas direcciones IP privadas simultáneamente.

Correlaciones de direcciones estáticas

En ocasiones, es posible que desee configurar una estación o un servidor en la red privada a la que pueda accederse directamente desde la red pública. En este caso, debe realizar una correlación estática de la dirección privada de la estación con una dirección pública determinada. Todos los mensajes salientes de la dirección privada se convierten a la dirección pública designada, mientras que todos los mensajes entrantes a la dirección pública designada se reenvían automáticamente a la dirección privada asociada. Hay dos clases de correlaciones de direcciones estáticas: NAT y NAPT.

Correlaciones de direcciones estáticas NAT

En una correlación NAT, todos los protocolos IP pueden acceder al sistema principal. Esto es un ejemplo de la configuración de una correlación NAT:

Dirección privada	10.1.1.2
Puerto privado	0
Dirección NAT pública	9.67.1.1
Puerto público	0

Correlación de direcciones estáticas NAPT

Para especificar una aplicación TCP o UDP, tiene la opción de especificar una correlación NAPT que incluya un puerto privado conocido públicamente. Para la correlación de direcciones estáticas NAPT, es preciso configurar una dirección pública NAPT. Por ejemplo, para configurar un sistema principal Telnet en la dirección privada 10.1.1.1 para que utilice la dirección pública NAPT 9.67.1.2, la correlación estática se configuraría de la manera siguiente:

Dirección privada	10.1.1.1
Puerto privado	23
Dirección NAPT pública	9.67.1.2
Puerto público	23

Los puertos privado y público se correlacionan con el puerto 23, que es el puerto conocido públicamente para Telnet. Por otra parte, si el administrador tiene también un servidor FTP (con la dirección conocida públicamente 21) en la misma dirección privada 10.1.1.1 que se correlaciona con la dirección pública NAPT 9.67.1.2, esta correlación puede tener el siguiente aspecto:

Utilización de la conversión de direcciones de red

Dirección privada	10.1.1.1
Puerto privado	21
Dirección NAPT pública	9.67.1.2
Puerto público	21

El servidor que tiene la dirección 10.1.1.1 tiene la misma dirección pública NAPT (9.67.1.2) para ambas aplicaciones, pero NAPT puede distinguir entre ambas utilizando números de puerto diferentes (23 y 21). No obstante, NAPT no puede distinguir entre dos servidores que utilicen la misma dirección pública NAPT y tengan el mismo número de aplicación y de puerto. Por ejemplo, si la dirección pública NAPT y el puerto conocido públicamente son los mismos para 10.1.1.3 puerto 21 y para 10.1.1.1 puerto 21, NAPT no puede distinguir si debe enviar el tráfico FTP de entrada al servidor 10.1.1.3 o al 10.1.1.1. Para configurar más de un servidor con la misma dirección NAPT y la misma aplicación, debe utilizar en el servidor un puerto distinto del conocido públicamente (por ejemplo, inicie el daemon FTP en el puerto 200).

Definición de filtros de paquetes y reglas de control de acceso para NAT

Además de identificar el rango de direcciones privadas que NAT o NAPT debe convertir, el administrador debe configurar los filtros de paquetes y las reglas de control de acceso para IP en el 2216. La configuración de NAT requiere que configure un filtro de paquetes de entrada y otro de salida en la interfaz conectada a la red pública. Tiene que configurar una o más reglas de control de acceso en el filtro de paquetes de entrada y también una o más de dichas reglas en el filtro de paquetes de salida. Las reglas de control de acceso de filtro de entrada pasan a NAT paquetes de entrada con las adecuadas direcciones públicas definidas. Las reglas de control de acceso de filtro de salida pasan a NAT paquetes de salida con las adecuadas direcciones privadas definidas.

Las reglas de control de acceso que se aplican para NAT tiene los tipos de reglas de control de acceso **I** y **N**, que corresponden a los tipos inclusivo y NAT. Consulte el manual *Consulta de configuración y supervisión de protocolos, Vol. 1* para obtener información acerca de la configuración de controles de acceso IP.

Nota: También se puede configurar NAT junto con un túnel de IPsec. En “Configuración de las reglas de control de acceso de filtros de paquetes para el direccionador A” en la página 407 se halla un ejemplo de esta configuración.

Ejemplo: Configuración de NAT con filtros IP y reglas de control de acceso

Este ejemplo indica cómo configurar NAT para el direccionador de apéndice en la red que se muestra en la Figura 42 en la página 473. Consulte “Configuración y supervisión de la Conversión de direcciones de red” en la página 477 para ver las descripciones de los mandatos.

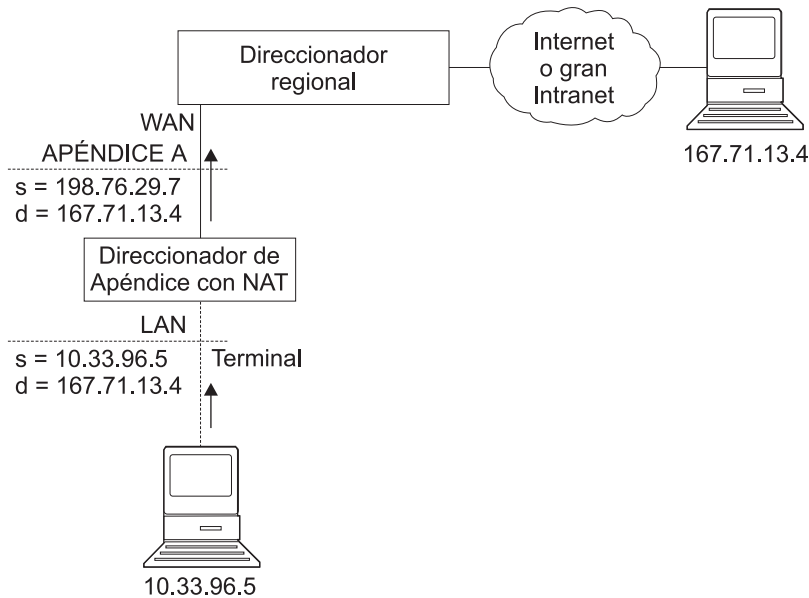


Figura 42. Red que ejecuta NAT

Siga este procedimiento:

1. Configure agrupaciones de direcciones públicas para que NAT y NAPT las utilice. Con este fin, utilice el mandato **reserve**.

```
NAT config> reserve No 198.76.29.7 255.255.255.0 6 pool1 198.76.29.7
NAT config> reserve No 198.76.29.15 255.255.255.0 3 pool1 0.0.0.0
```

En este ejemplo, se establece una agrupación denominada *pool1*. La dirección NAPT de la agrupación es 198.76.29.7. Las direcciones 198.76.29.13 y 198.76.29.14 no están disponibles, por lo que la agrupación está configurada para excluirlas. Los parámetros entrados son: *dirección pública*, *máscara*, *número en grupo*, *nombre* y *dirección NAPT*. El valor 0.0.0.0 para la dirección NAPT significa que ninguna dirección de este grupo es la dirección NAPT. Utilice 0.0.0.0 para la dirección NAPT en todos los grupos, si no configura NAPT para la agrupación.

2. Utilice el mandato **translate** para establecer los rangos de direcciones privadas que las direcciones públicas de *pool1* deben convertir. Los parámetros entrados son: *dirección privada*, *máscara* y *nombre*.

```
NAT config> translate 10.33.96.0 255.255.255.0 pool1
```

3. Defina correlaciones estáticas para las estaciones en la red privada que se deben correlacionan de forma permanente con una de las direcciones públicas. Los mandatos siguientes identifican una máquina (10.33.96.5) que recibirá cualquier tipo de tráfico procedente de la red pública. Una segunda máquina (10.33.96.4) es un servidor Telnet y HTTP a la vez. Los parámetros son *dirección privada*, *número de puerto privado*, *dirección pública* y *número de puerto público*. Tenga en cuenta que la dirección NAPT para *pool1* se utiliza como dirección pública para el sistema principal configurado con dos números de puerto.

```
NAT config> map 10.33.96.5 0 198.76.29.8 0
NAT config> map 10.33.96.4 23 198.76.29.7 23
NAT config> map 10.33.96.4 80 198.76.29.7 80
```

4. Habilite NAT.

Utilización de la conversión de direcciones de red

```
NAT config> enable NAT
```

5. Cree dos filtros de paquetes IP, de manera que IP pase los paquetes a NAT. Son los filtros de paquetes de entrada y salida para la interfaz 0, que es la que está conectada a la red pública.

```
IP Config> add packet-filter outbound out-0 0  
IP Config> add packet-filter inbound in-0 0
```

6. Utilice el mandato **update** para que aparezca el indicador `packet-filter 'filter-name'` Config>. Añada una regla de control de acceso para NAT al filtro de entrada. Se deben pasar a NAT los paquetes recibidos a través de la interfaz pública (net 0) que están destinados a una dirección de la agrupación de direcciones públicas reservadas de NAT. NAT sustituirá la dirección pública (y el puerto público, si el paquete está destinado a la dirección NAPT) por la dirección privada correcta (y el puerto privado, si el paquete está destinado a la dirección NAPT). La dirección y máscara 0.0.0.0 para la dirección de origen Internet indican que las direcciones de origen de la red pública se pasarán a NAT.

```
IP Config>update packet-filter  
Packet-filter name [ ]? in-0  
Packet-filter 'in-0' Config> add access  
Enter type [E]? IN  
Internet source [0.0.0.0]?  
Source mask [255.255.255.255]? 0.0.0.0  
Internet destination [0.0.0.0]? 198.76.29.0  
Destination mask [255.255.255.255]?255.255.255.0  
Enter starting protocol number ([0] for all protocols) [0]?  
Enable logging? (Yes or [No]):  
Packet-filter 'in-0' Config>
```

El rango de direcciones de la regla de control de acceso es mayor que el rango de direcciones definidas en pool1. Si la dirección del paquete pasada a NAT se encuentra dentro del rango definido en la regla de control de acceso, pero no pertenece a la agrupación de direcciones públicas, NAT devuelve el paquete a IP sin efectuar modificaciones.

7. Si desea que el direccionador pase los paquetes que no cumplen la regla de control de acceso, en lugar de eliminarlos, puede crear una regla de control de acceso con comodín. El siguiente ejemplo muestra una regla de control de acceso con estas características:

```
Packet-filter 'in-0' Config> add access  
Enter type [E]? I  
Internet source [0.0.0.0]? 0.0.0.0  
Source mask [255.255.255.255]? 0.0.0.0  
Internet destination [0.0.0.0]? 0.0.0.0  
Destination mask [255.255.255.255]?0.0.0.0  
Enter starting protocol number ([0] for all protocols) [0]?  
Enable logging? (Yes or [No]):  
Packet-filter 'in-0' Config>
```

8. Añada una regla de control de acceso para NAT al filtro de paquetes de salida. Los paquetes que se deben reenviar desde la interfaz net 0 que tengan una dirección de origen en la red privada, se identifican para que IP pueda pasarlos a NAT. NAT sustituye la dirección privada por una de las direcciones públicas de pool1.

```
Packet-filter 'out-0' Config> add access  
Enter type [E]? IN  
Internet source [0.0.0.0]? 10.33.96.0  
Source mask [255.255.255.255]? 255.255.255.0  
Internet destination [0.0.0.0]?  
Destination mask [255.255.255.255]?0.0.0.0  
Enter starting protocol number ([0] for all protocols) [0]?  
Enable logging? (Yes or [No]):  
Packet-filter 'out-0' Config>
```

Con este filtro de paquetes, al igual que con el filtro *in-0*, puede añadir una regla de control de acceso inclusiva con comodín como última regla de control de acceso, si piensa reenviar los paquetes que no cumplan la regla de control de acceso.

9. Puede utilizar el mandato **list packet-filter nombre-filtro** en el indicador IP Config> para comprobar la exactitud y la secuencia de las reglas de control de acceso en cada filtro de paquetes.

10. Habilite los controles de acceso para IP.

```
IP Config> set access-control on
```

11. Restablezca IP y NAT utilizando talk 5. Hasta ahora, el usuario ha creado modificaciones en la configuración de direccionador, pero estos cambios no han afectado al direccionador. Los mandatos de restablecimiento para IP y NAT causan que el direccionador lea la nueva configuración, y se ejecutan con las reglas definidas en la configuración.

```
NAT> reset NAT  
IP> reset IP
```


Configuración y supervisión de la Conversión de direcciones de red

Este capítulo describe los mandatos de configuración y supervisión de la Conversión de direcciones de red (NAT) e incluye las secciones siguientes:

- “Acceso al entorno de configuración de la Conversión de direcciones de red”
- “Mandatos de configuración de la Conversión de direcciones de red”
- “Acceso al entorno de supervisión de la Conversión de direcciones de red” en la página 484
- “Mandatos de supervisión de la Conversión de direcciones de red” en la página 484

Acceso al entorno de configuración de la Conversión de direcciones de red

Para acceder al entorno de configuración de NAT, entre el siguiente mandato en el indicador Config>:

```
Config> feature nat
Network Address Protocol user configuration
NAT config>
```

Mandatos de configuración de la Conversión de direcciones de red

Esta sección explica los mandatos de configuración de la Conversión de direcciones de red (NAT). Para configurar NAT, entre estos mandatos en el indicador NAT config>.

Tabla 58. Mandatos de configuración de NAT

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxiv.
Change	Cambia las agrupaciones de reserva de direcciones IP públicas, los rangos de conversión de direcciones privadas y las correlaciones estáticas.
Delete	Suprime las agrupaciones de reserva de direcciones IP públicas, los rangos de conversión de direcciones privadas y las correlaciones estáticas.
Disable	Inhabilita NAT.
Enable	Habilita NAT.
List	Lista información acerca de la configuración de NAT.
Map	Crea un vínculo estático NAT o NAPT para una estación o un servidor.
Reserve	Crea una agrupación de direcciones IP públicas y añade direcciones a dicha agrupación.
Reset	Hace que el direccionador lea la configuración de NAT y se ejecute según las normas de NAT que se han configurado.
Set	Define los tiempos de espera.
Translate	Identifica las direcciones IP privadas que la agrupación de direcciones públicas de NAT debe convertir.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiv.

Change

Utilice el mandato **change** para modificar las agrupaciones de reserva de direcciones IP públicas, los rangos de conversión de direcciones IP privadas y las correlaciones estáticas.

Sintaxis:

```
change          reserve
                  translate
                  mappings
```

reserve *agrupaciones*

Proporciona indicadores que le permiten modificar las características de cualquier agrupación de reserva de direcciones IP públicas (tales como direcciones y máscaras IP).

Valores válidos: un número de índice que sirve para identificar la agrupación configurada. Este número se visualiza al entrar el mandato **list reserve pools**.

Valor por omisión: ninguno

translate *rangos*

Proporciona indicadores que le permiten modificar las características de cualquier rango de conversión de direcciones IP privadas (tales como direcciones y máscaras IP).

Valores válidos: un número de índice que identifique el rango de conversión configurado. Este número se visualiza al entrar el mandato **list translate**.

Valor por omisión: ninguno

mappings

Proporciona indicadores que le permiten modificar las características de cualquier correlación de direcciones estáticas (tales como direcciones IP y puertos).

Valores válidos: un número de índice que identifique la correlación configurada. Este número se visualiza al entrar el mandato **list mappings**.

Valor por omisión: ninguno

Delete

Utilice el mandato **delete** para suprimir las agrupaciones de reserva de direcciones IP públicas, los rangos de conversión de direcciones IP privadas y las correlaciones.

Sintaxis:

```
delete          reserve
                  translate
                  mappings
```

reserve *agrupaciones*

Proporciona indicadores que le permiten suprimir cualquier agrupación de reserva de direcciones IP públicas.

Valores válidos: un número de índice que sirve para identificar la agrupación configurada. Este número se visualiza al entrar el mandato **list reserve pools**.

Valor por omisión: ninguno

translate *rangos*

Proporciona indicadores que le permiten suprimir cualquier rango de conversión de direcciones IP privadas.

Valores válidos: un número de índice que identifique el rango de conversión configurado. Este número se visualiza al entrar el mandato **list translate**.

Valor por omisión: ninguno

mappings

Proporciona indicadores que le permiten suprimir cualquier correlación de direcciones estáticas.

Valores válidos: un número de índice que identifique la correlación configurada. Este número se visualiza al entrar el mandato **list mappings**.

Valor por omisión: ninguno

Disable

Utilice el mandato **disable** para inhabilitar AT. Puede inhabilitar NAT para que elimine los paquetes que requieren conversión o para que los pase.

Sintaxis:

disable nat

drop

pass

drop

Inhabilita NAT para que elimine los paquetes que requieren conversión.

pass

Inhabilita NAT para que pase los paquetes que requieren conversión.

Enable

Utilice el mandato **enable** para habilitar NAT. La habilitación de NAT la prepara para su ejecución, pero no se ejecutará hasta que utilice el mandato **reset** o reinicie el direccionador.

Sintaxis:

enable nat

List

Utilice el mandato **list** para listar las agrupaciones de reserva de direcciones IP públicas, los rangos de conversión de direcciones IP privadas, las correlaciones, los valores globales y toda la información de NAT.

Sintaxis:

list

reserve

addresses

Configuración de la Conversión de direcciones de red (Talk 6)

pools
translate
mappings
global
all

En el ejemplo siguiente, el tiempo se visualiza como horas, minutos y segundos. La antigüedad de la entrada es el tiempo transcurrido desde que se utilizó la entrada por última vez. Un vínculo indica que existe tráfico entre estas dos direcciones. Los tiempos de espera determinan cuánto tiempo transcurrirá después de la última comunicación antes de eliminar un vínculo. Consulte el mandato **set** para obtener más información acerca de los tiempos de espera.

Ejemplo:

```
NAT config>list all
NAT Globals:
NAT is ENABLED
Tcp Timeout....: 24:00:00
Non-Tcp Timeout: 0:01:00
NAT Reserved Address Pool(s):
Index First Address      Mask          Count NAPT Address  Pool Name
1    9.8.7.1             255.255.255.0  3    0.0.0.0       pool1
2    9.8.7.6             255.255.255.0  12   9.8.7.9       pool1
NAT Translate Range(s):
Index IP Address          IP Mask          Associated Pool Name
1    7.1.1.0               255.255.255.0   pool1
2    10.0.0.0              255.0.0.0       pool1
NAT Static Mapping(s):
Index Private Address:Port  Public Address.:Port
1    10.1.2.3              0    9.8.7.1          0
2    7.1.1.1               21   9.8.7.9          21
```

Map

Utilice el mandato **map** para vincular estadísticamente un sistema principal o un servidor de la red privada a una dirección pública. Este mandato, que se puede utilizar para configurar servidores en la red privada, establece una asociación al arrancar NAT que no cambia nunca.

Las correlaciones estáticas con el número de puerto público y privado 0 son valores de NAT: las que tienen otros valores para los números de puerto son correlaciones NAPT.

Sintaxis:

```
map          dirección-privada número-puerto-privado dirección-pública  
              número-puerto-público
```

dirección-privada

Dirección privada de la estación de trabajo.

Valores válidos: una dirección de sistema principal Internet con formato IP válido. Debe ser la dirección asignada a una estación de la red de apéndice que requiere tener acceso permanente desde la red pública, como un servidor.

Valor por omisión: ninguno

número-puerto-privado

Número de puerto TCP/UDP de la aplicación que se ejecuta en el dispositivo con la dirección privada. Entrar **0** crea un vínculo NAT, mientras que entrar otro valor crea un vínculo NAPT. Los valores comunes de puerto para NAPT son 23 para Telnet, 21 para FTP y 80 para HTTP.

Valores válidos: 0 - 65535

Valor por omisión: 0

dirección-pública

La dirección IP pública con la que se debe correlacionar esta dirección privada. Debe ser una dirección NAPT para una correlación NAPT y una dirección NAT para una correlación NAT.

Valores válidos: una dirección IP válida que sea exclusiva en la red pública. La red pública puede ser Internet o una intranet, según el diseño de la red.

Valor por omisión: ninguno

número-puerto-público

Número de puerto de los paquetes que se deben convertir en la dirección pública. El valor 0 representa todas las puertos. Los valores comunes de puerto son 23 para Telnet, 21 para FTP y 80 para HTTP.

Valores válidos: 0 - 65535

Valor por omisión: 0

En este ejemplo, el servidor con la dirección IP privada 10.11.12.200 acepta todo el tráfico de Internet; el servidor con la dirección privada 10.11.12.199 es un servidor Telnet y FTP.

Ejemplo:

```
map 10.11.12.200 0 9.8.7.2 0
map 10.11.12.199 23 9.8.7.9 23
map 10.11.12.199 21 9.8.7.9 21
```

Reserve

Utilice el mandato **reserve** para crear y añadir un rango de direcciones IP a una agrupación de direcciones públicas. Además, puede utilizarse para añadir una interfaz de IP dinámico a la agrupación de direcciones públicas.

Sintaxis:

```
reserve dinámica
           [interfaz][dirección-pública][máscara][número-en-grupo] nombre
           [dirección-napt]
```

Nota: La visualización de los valores indicados entre corchetes es opcional.

- **Dinámica** - Especifica si esta entrada corresponde a un grupo de direcciones público o a una interfaz de Dirección dinámica que recuperará su dirección IP de una conexión PPP que utiliza IPCP. Los valores válidos son *yes* o *no*. El valor por omisión es *no*. Si *Dinámica=yes*, sólo tiene que especificar la interfaz y el nombre. Si *Dinámica=no*, no especifique la interfaz, pero tendrá que especificar todos los demás valores.

Configuración de la Conversión de direcciones de red (Talk 6)

- Interfaz - Especifica la interfaz de Dirección dinámica tal como está configurada en IP. Puede especificarse cualquier número de interfaz válido. El valor por omisión es cero.

dirección-pública

La primera dirección IP pública de la secuencia de direcciones que compone este rango o grupo de la agrupación. Por ejemplo, si este grupo de la agrupación incluye las 12 direcciones en secuencia, desde la 9.8.7.6 a la 9.8.7.17, este valor es 9.8.7.6.

Nota: Para añadir otro rango de direcciones a la agrupación de direcciones públicas, utilice el mandato **reserve** de manera separada para cada grupo, relacionando un grupo con otro mediante el mismo nombre de agrupación. Por ejemplo, las direcciones 9.8.7.6 a 9.8.7.17 pueden configurarse en un solo grupo dentro de la agrupación pool1, mientras que las direcciones 9.8.7.1 a 9.8.7.3 pueden configurarse en otro grupo dentro de esa misma agrupación. En tal caso, esta agrupación no configura o no utiliza las direcciones 9.8.7.4 y 9.8.7.5.

Valores válidos: una dirección IP válida que sea exclusiva en la red pública

Valor por omisión: ninguno

máscara

Una máscara para seleccionar bits de la dirección IP. La máscara, como una dirección Internet, tiene una longitud de 32 bits. Los 1 que aparecen en la máscara seleccionan la parte de la red o subred de la dirección. Los 0 seleccionan la parte del sistema principal. Por ejemplo, la dirección 9.8.7.6 y la máscara 255.255.0.0 incluyen el rango de todas las direcciones cuyos dos primeros bytes son 9.8 (es decir, de 9.8.0.0 a 9.8.255.255).

Valores válidos: cualquier máscara IP válida

Valor por omisión: ninguno

número-en-grupo

Especifica cuántas direcciones secuenciales, empezando por *dirección-pública*, están incluidas en el grupo. Para las direcciones 9.8.7.6 a 9.8.7.17, este valor es 12.

Valores válidos: 1 - el valor que la máscara IP puede definir

Valor por omisión: ninguno

nombre

El nombre de la agrupación de reserva de direcciones públicas. Esta serie tiene que coincidir con el nombre de agrupación en el mandato **translate** correspondiente.

Valores válidos: cualquier nombre, utilizando un máximo de 16 caracteres imprimibles; los blancos iniciales y de cola se pasan por alto.

Valor por omisión: ninguno

dirección-napt

La única dirección IP de la agrupación de direcciones públicas que será utilizada por la Conversión de puertos de direcciones de red (NAPT). Esta dirección se utiliza para que el tráfico TCP y UDP correlacione varias direcciones privadas con una dirección NAPT pública, según el número de puerto de protocolo. La utilización de NAPT es opcional. Si se utiliza, sólo puede haber

Configuración de la Conversión de direcciones de red (Talk 6)

una dirección NAPT por agrupación de direcciones públicas. Si no hay ninguna dirección NAPT para una agrupación o un grupo, entre el valor **0.0.0.0**. Sólo tiene que entrar la dirección NAPT una vez para la agrupación.

Valores válidos: una de las direcciones IP públicas. No es necesario que esté incluida en el rango de valores definidos en la agrupación de direcciones públicas, pero debe estar en la misma subred.

Valor por omisión: 0.0.0.0 (quiere decir que no hay NAPT)

Ejemplo:

```
reserve no 9.8.7.1 255.255.255.0 3 pool1 0.0.0.0
reserve no 9.8.7.6 255.255.255.0 12 pool1 9.8.7.9
reserve yes 2 dynamic_ip_pool
```

Reset

Utilice el mandato **reset** para restablecer NAT. Este mandato suprime todos los vínculos, libera toda la memoria utilizada por NAT y reinicia NAT según la configuración actual de Talk 6. El restablecimiento de NAT no altera ningún otro componente del 2216.

Sintaxis:

reset nat

Observe que, si NAT encuentra una configuración no válida, verá un mensaje al respecto. Revise los mensajes ELS de NAT para ver el motivo de la anomalía en la inicialización de NAT.

Set

Utilice el mandato **set** para definir tiempos de espera TCP y no TCP.

Sintaxis:

set tcp
nontcp

tcp *tiempo-espera*

Tiempo que NAT mantiene un vínculo TCP después de que el último mensaje pase entre dos estaciones de trabajo vinculadas. Un vínculo es el mantenimiento de la relación entre una dirección privada y una de las direcciones IP públicas.

Valores válidos: 0 - 65535 minutos (de 0 minutos a unos 45 días)

Valor por omisión: 1440 minutos (24 horas)

nontcp *tiempo-espera*

Tiempo que NAT mantiene un vínculo que no es TCP después de que el último mensaje pase entre dos estaciones de trabajo vinculadas. Un vínculo es el mantenimiento de la relación entre una dirección privada y una de las direcciones IP públicas.

Valores válidos: 0 - 65535 minutos (de 0 minutos a unos 45 días)

Valor por omisión: 1 minuto

Translate

Utilice el mandato **translate** para añadir una subred a la lista de direcciones que NAT convertirá. Cada subred es un rango de conversión. Es preciso entrar este mandato una vez por cada rango de conversión que NAT debe conocer. Un número cualquiera de rangos de conversión pueden utilizar una única agrupación de reserva de direcciones públicas.

Sintaxis:

```
translate dirección-privada máscara nombre
```

dirección-privada

Cualquier dirección IP de sistema principal o de subred que debe convertirse.

Valores válidos: una dirección en formato IP decimal punteado válido.

Cuando se ejecuta AND con su máscara de subred, esta dirección identifica todas las direcciones que existen en una subred de apéndice. Una subred de apéndice es una red que sólo accede a la red pública a través del direccionador.

Valor por omisión: ninguno

máscara

Valores válidos: la máscara de red o subred asociada a la red de apéndice que se debe convertir.

Valor por omisión: máscara de clase de la dirección privada

nombre

El nombre de la agrupación de direcciones públicas que NAT debe utilizar para este rango de direcciones privadas.

Valores válidos: cualquier nombre, utilizando un máximo de 16 caracteres imprimibles. Debe coincidir con un nombre de agrupación de direcciones públicas que se haya creado con el mandato **reserve**.

Valor por omisión: ninguno

Acceso al entorno de supervisión de la Conversión de direcciones de red

Para acceder al entorno de supervisión de NAT, escriba

```
* t 5
```

A continuación, entre el siguiente mandato en el indicador **+**:

```
+ feature NAT  
NAT>
```

Aparecerá el indicador NAT>.

Mandatos de supervisión de la Conversión de direcciones de red

Esta sección describe los mandatos de supervisión de la Seguridad de IP. Entre estos mandatos en el indicador NAT>.

Tabla 59. Mandatos de supervisión de NAT

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxiv.
List	Lista información acerca de NAT.
Reset	Hace que el direccionador lea la configuración de NAT y se ejecute según las normas de acceso de NAT que se han configurado. NAT no afecta a la ejecución del direccionador hasta que se entra el mandato reset NAT .
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiv.

List

Utilice el mandato **list** para visualizar información acerca de la configuración de NAT.

Sintaxis:

```
list          all
              binding
              fragment
              global
              reserve
                pools
                addresses
              statistics
              translate
```

En el ejemplo siguiente, el tiempo se visualiza como horas, minutos y segundos. La antigüedad de la entrada es el tiempo transcurrido desde que se utilizó la entrada por última vez. Un vínculo indica que se ha establecido una sesión entre estas dos direcciones. Los tiempos de espera determinan cuánto tiempo transcurrirá después de la última comunicación antes de eliminar un vínculo. Consulte el mandato **set** de Talk 6 para obtener más información acerca de los tiempos de espera.

Supervisión de la Conversión de direcciones de red

Ejemplo:

```
NAT>list all
NAT Globals:
Current State      Tcp Timeout      Non-Tcp Timeout  Memory Usage (in bytes)
ENABLED           24:00:00        0:01:00         408

NAT Statistics:
Requests :      Passes      Drops      Holds
0 :          0            0          0

NAT Address Binding(s):
Private Address//Port  Public Address//Port  Bind Type  Entry Age
7.1.1.1 21            9.1.1.1 21  STATIC    0:00:13
10.1.2.3 0              9.1.1.2 0  STATIC    0:00:13

NAT TCP Session Information:
Private Address//Port  Public Address//Port  Tcp State  Data Delta  Entry Age
7.1.1.1 21            9.1.1.1 21  ESTAB'ED   0          0:00:56

NAT Translate Range(s):
Base Ip Address      Range Mask      Associated Reserve Pool
7.1.1.0             255.255.255.0  carol
10.0.0.0            255.0.0.0     carol

NAT Reserve Pool(s):
Reserve Pool      Pool Size      NAPT Address  1st Available Address
carol             21            9.1.1.1      9.1.1.12
-----
Number of Reserve Pools using NAPT.....: 1
Number of configured Reserved Addresses: 21

NAT Fragment Information:
Number of Entries      Number of Saved Fragments
0                      0
```

Reset

Utilice el mandato **reset** para restablecer NAT. Este mandato suprime todos los vínculos, libera toda la memoria utilizada por NAT y reinicia NAT según la configuración actual de Talk 6. El restablecimiento de NAT no altera ningún otro componente del 2216.

Sintaxis:

reset nat

Utilización de un Acceso de marcación de entrada a las LAN (DIALs) Server

Un Servidor DIAL permite que los usuarios remotos se conecten mediante una marcación de entrada a una LAN y accedan a sus recursos de la misma manera que si estuvieran conectados localmente con un adaptador de LAN.

El IBM DIAL Dial-In Client se ejecuta en la estación de trabajo remota y proporciona la función de marcación de entrada. La Figura 43 muestra un ejemplo de un dispositivo utilizado como un Servidor DIAL que da soporte a la función de marcación de entrada.

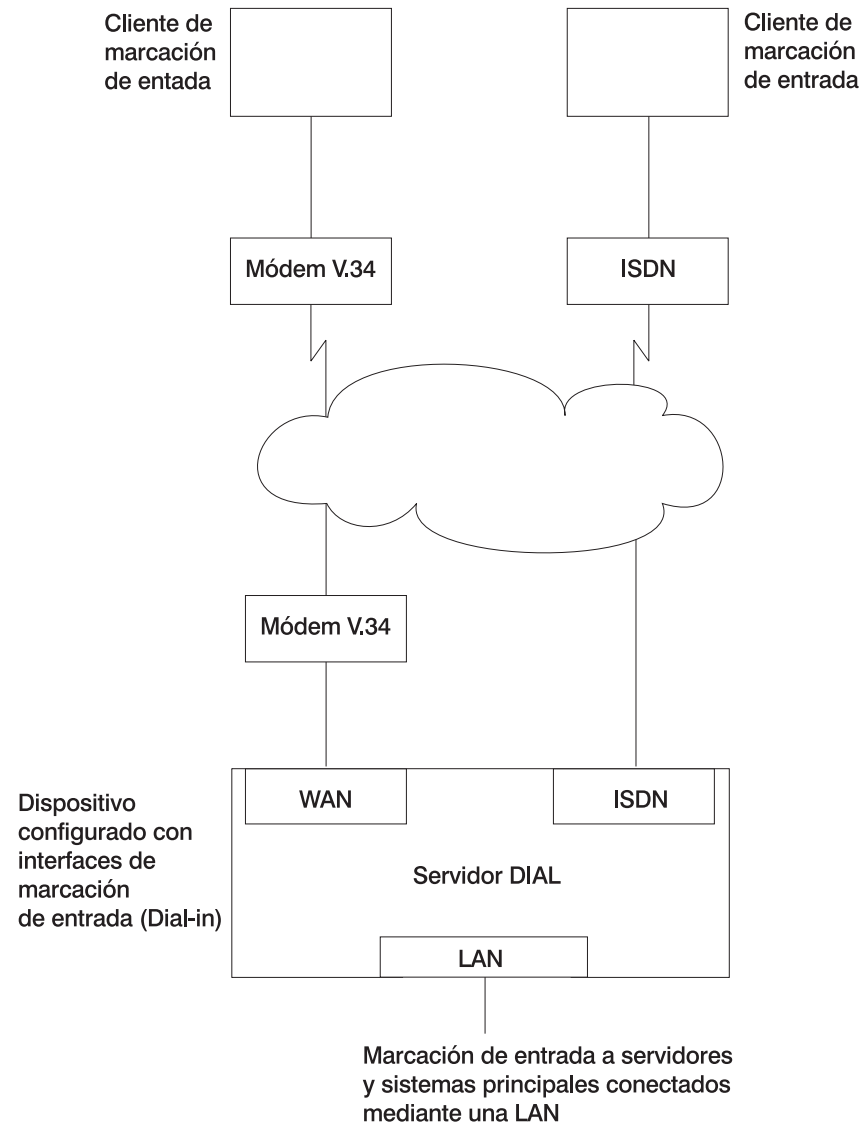


Figura 43. Ejemplo de un Servidor DIAL dando soporte a marcación de entrada

Nota: El 2216 no da soporte a las interfaces de marcación de salida.

Antes de utilizar Dial-In-Access

Antes de utilizar Dial-In Access, necesita:

- Una estación de trabajo que ejecute el IBM DIAL Dial-In Client u otro cliente PPP de marcación de entrada (al que se hace referencia como **cliente de marcación de entrada** o **cliente PPP de marcación de entrada** a lo largo de las secciones siguientes).
- Configuraciones de protocolos completadas en la máquina cliente.
- Línea(s) PRI RDSI conectada(s) al 2216 que desea utilizar para la marcación de entrada de usuario único.
- Un Servidor DIAL totalmente configurado en la LAN.

Configuración del acceso de marcación de entrada

Esta sección describe cómo configurar la función de marcación de entrada en el Servidor DIAL. La configuración de un cliente para utilizar el acceso de marcación de entrada se describe en la documentación asociada con el cliente que utiliza la estación de trabajo.

Configuración de interfaces de marcación de entrada

Las interfaces de marcación de entrada en el 2216 son un tipo especial de circuito de marcación. Dado que la mayoría de los valores para un circuito de marcación típico no son relevantes para las aplicaciones de marcación de entrada de usuario único, puede añadirse un nuevo tipo de dispositivo, denominado **de marcación de entrada**, que defina los valores por omisión adecuados para el circuito de marcación. La adición de un dispositivo de marcación de entrada también configura los valores por omisión de configuración del encapsulador PPP que funcionan con la mayoría de clientes PPP de marcación de entrada, incluido el IBM DIAL Dial-In Client. Estos valores por omisión están descritos en las secciones “Valores por omisión de los parámetros del circuito de marcación para las interfaces de marcación de entrada” y “Parámetros de encapsulador PPP de circuito de marcación para los circuitos de marcación de entrada” en la página 489.

Nota: La función DIALs sólo se puede habilitar en los circuitos de marcación de entrada. Los circuitos de marcación de entrada sólo están soportados cuando la red de base es una red RDSI.

Valores por omisión de los parámetros del circuito de marcación para las interfaces de marcación de entrada

Notas:

1. No realice una alteración temporal de los parámetros descritos en esta sección. Hacerlo impediría que la función de marcación de entrada operase correctamente.
2. Algunos parámetros no se pueden visualizar o no son configurables. Para obtener una descripción completa de los parámetros, consulte “Configuring and Monitoring Dial Circuits” en el manual *Nways Multiprotocol Access Services Guía del usuario de software*.

Los siguientes valores por omisión se definen al añadir una interfaz de marcación de entrada:

- El **tiempo desocupado (idle time)** se establece a 0. Observe que un circuito estándar se define como un circuito en el que el temporizador de desocupado no tiene sentido. No será un circuito fijo para realizar la marcación de salida automática. La única vez que el circuito realizará la marcación de salida se produce si se ha negociado una devolución de llamada PPP, o si el PPP multienlace se ha habilitado en este circuito. Consulte “Shiva Password Authentication Protocol (SPAP)” y “Using the Multilink PPP Protocol” en el manual *Nways Multiprotocol Access Services Guía del usuario de software*.
- Las **llamadas de entrada (inbound calls)** están permitidas. Se configura cualquier llamada de entrada, porque los clientes PPP de marcación de entrada no utilizan el intercambio de LID implementado por los circuitos de marcación de Nways.
- Las **llamadas de salida (outbound calls)** están permitidas.
- Se configura una dirección de destino por omisión para “default_address”. Esta dirección se añade a la lista de direcciones RDSI. Dado que estas llamadas son de entrada y las únicas llamadas de salida serán el resultado de una devolución de llamada o un intercambio PPP de multienlace, la dirección de destino no tiene sentido. No obstante, la dirección es necesaria para los parámetros de circuito. No suprima esta dirección o los circuitos quedarán inhabilitados.

Parámetros de encapsulador PPP de circuito de marcación para los circuitos de marcación de entrada

Nota: Para obtener una descripción completa de los siguientes parámetros, consulte “Using Point-to-Point Protocol Interfaces” en el manual *Nways Multiprotocol Access Services Guía del usuario de software*.

Los siguientes valores por omisión se definen al añadir una interfaz de marcación de entrada:

- La autenticación se habilita para SPAP, CHAP y PAP.
- La MRU PPP se define como 1522. Este tamaño de MRU es necesario para las versiones Windows 3.1, OS/2 y DOS de los IBM DIAL Dial-In Clients. No cambie este valor, a menos que sepa que no utiliza estos clientes.
- Habilita automáticamente DIAL en el encapsulador PPP. Esto activa algunas características importantes para los usuarios de Acceso de marcación de entrada a las LAN, como el protocolo NetBIOS Control, el protocolo NetBIOS Frame Control, el tiempo restante, la autenticación SPAP, la devolución de llamada, la identificación de LCP y la adición y supresión automáticas de rutas IP estáticas al cliente. Consulte “Using Point-to-Point Protocol Interfaces” en el manual *Nways Multiprotocol Access Services Guía del usuario de software* para obtener más información sobre las características de DIALs.

Adición de una interfaz de marcación de entrada

Para añadir una interfaz de marcación de entrada:

1. Configure una red de base RDSI disponible en el 2216. Consulte la información sobre configuración en “Using the ISDN Interface” del manual *Nways Multiprotocol Access Services Guía del usuario de software*.
2. Entre **talk 6** para acceder al indicador Config >.
3. Entre **add device dial-in** en el indicador Config> para añadir la interfaz de marcación de entrada. Se le preguntará cuántos circuitos de marcación de

Utilización de DIALs

entrada se deben añadir. Este mandato creará las nuevas redes, informará de sus números de red, solicitará el número de red de base y solicitará la habilitación de PPP Multienlace.

Ejemplo: suponga que la red máxima actual es 1 y desea añadir dos redes de marcación de entrada a la red de base 1.

La Figura 44 es un ejemplo de definición de interfaz de marcación de entrada.

Figura 44. Adición de una interfaz de marcación de entrada

```
*talk 6
Config>add device dial-in
Enter the number of PPP Dial-in Circuit interfaces [1]? 2
Adding devices as interfaces 2-3
Defaulting data-link protocol to PPP

Base net for this circuit [0]? 1
Enable as a Multilink PPP link? [no]
Disabled as a Multilink PPP link.

Base net for this circuit [0]? 1
Enable as a Multilink PPP link? [no]
Disabled as a Multilink PPP link.

Use "set data-link" command to change the data-link protocol
Use "net " command to configure dial circuit parameters.
Config>li dev
Ifc 0   Ethernet                               Slot: 1   Port 1
Ifc 1   8-port ISDN Primary T1/J1             Slot: 4   Port 1
Ifc 2   PPP Dial-in Circuit
Ifc 3   PPP Dial-in Circuit
```

Utilización de módem nulo

Al utilizar un módem nulo, utilice el handshake completo D25NM-3:

Correlación de patillas:

1 a 1	1 a 1
2 a 3	3 a 2
4 a 5	5 a 4
6 a 8, 20	8, 20 a 6
7 a 7	7 a 7

Antes de configurar los parámetros globales de DIAL

Esta sección describe los parámetros globales de Servidor DIAL.

Direcciones IP proporcionadas por el servidor

Se puede configurar el direccionador para proporcionar una dirección IP para que un cliente de la marcación de entrada la utilice mientras dure su conexión. La dirección que el direccionador asignará al cliente puede recuperarse mediante 4 métodos diferentes. Estos métodos se listan a continuación, por orden de prioridad:

1. ID de usuario

Una dirección IP se puede almacenar en el perfil de usuario PPP para cada cliente. Cuando un cliente se conecte y solicite una dirección IP, el

direccionador recuperará la dirección configurada en el perfil de usuario PPP del usuario. Esto permite al usuario obtener siempre la misma dirección IP, pero requiere una dirección IP exclusiva para cada usuario.

Utilice el mandato Config> **add ppp-user** para configurar una dirección IP en el perfil de usuario PPP.

2. Interfaz

Una dirección IP se puede almacenar en la configuración de interfaz de marcación de entrada. Cuando un cliente se conecte y solicite una dirección IP, el direccionador recuperará la dirección de la interfaz a través de la cual se ha establecido la conexión. Este método requiere una dirección IP exclusiva para cada interfaz de marcación de entrada.

Para definir la dirección IP de interfaz:

- Utilice el mandato Config> **list devices** para visualizar el número de interfaz asignado a la interfaz de hardware.
- Utilice el mandato Config> **net 'x'**, donde 'x' es el número de interfaz configurado, para acceder al indicador de mandatos para la interfaz.
- Utilice el mandato PPP Config> **set ipcp** para definir la dirección IP de interfaz.

3. Agrupación

Pueden almacenarse bloques de direcciones IP en una agrupación de direcciones IP. Cuando un cliente se conecte y solicite una dirección, el direccionador recuperará una dirección de la agrupación. Cuando el cliente se desconecte, la dirección regresará a la agrupación. Este método proporciona una única ubicación para configurar la dirección IP de un cliente de marcación de entrada, sin necesidad de un servidor de direcciones.

Utilice el mandato DIALs config> **add ip-pool** para añadir una agrupación de direcciones IP.

4. DHCP Proxy

Se puede alquilar una dirección IP desde un servidor DHCP. Cuando un cliente se conecte y solicite una dirección, el direccionador solicitará una dirección del servidor DHCP en nombre del cliente. Este método requiere que haya un servidor DHCP en la LAN o se configure en el direccionador. Un servidor DHCP puede proporcionar direcciones para los clientes en varios direccionadores. Consulte "DHCP (Dynamic Host Configuration Protocol)" en la página 492 para obtener más información.

Utilice el mandato DIALs config> **add dhcp-server** para añadir un servidor DHCP.

Métodos de asignación de direcciones IP

La dirección IP utilizada por un cliente de marcación de entrada mientras dure la conexión, puede proceder de 5 orígenes distintos. Estos orígenes se listan por orden de preferencia:

1. proporcionada por el cliente
2. asignada por el ID de usuario
3. asignada por la interfaz
4. agrupación de direcciones

5. servidor DHCP

Cuando un cliente de marcación de entrada se conecta, el direccionador recorre estos orígenes hasta que encuentra una dirección o agota todos los orígenes. Si no se puede encontrar ninguna dirección IP, la negociación de IPCP falla. Puede utilizarse cualquier combinación de métodos.

La configuración por omisión es:

```
Client      : Enabled
UserID     : Enabled
Interface  : Enabled
Pool       : Enabled
DHCP Proxy : Disabled
```

Nota: No hay direcciones configuradas por omisión en el perfil de usuario PPP, la interfaz o la agrupación de direcciones IP.

DHCP (Dynamic Host Configuration Protocol)

DHCP (Dynamic Host Configuration Protocol) se ha desarrollado para proporcionar parámetros de configuración a los sistemas principales de una red. Entre otros parámetros de configuración, DHCP tiene un mecanismo de asignación de direcciones de red a los sistemas principales.

La característica Proxy DHCP actúa como cliente *en nombre de* un usuario PPP de marcación de entrada. Esto permite que el dispositivo obtenga un alquiler de dirección IP mientras dure la sesión de marcación de entrada, o hasta que el alquiler caduque. La dirección IP que se asigna del servidor DHCP se comunica con el cliente de marcación de entrada a través de PPP IPCP (consulte "IP Control Protocol" en el manual *Nways Multiprotocol Access Services Guía del usuario de software* para obtener una descripción de IPCP). El software de cliente de marcación de entrada no sabe que se ha utilizado DHCP para asignar una dirección IP y, por lo tanto, no requiere ninguna activación de DHCP de ningún tipo.

El Proxy DHCP requiere que, por lo menos, se configure un servidor DHCP y sea accesible desde el direccionador.

El Proxy DHCP requiere que las direcciones asignadas a los usuarios de marcación de entrada estén en la misma subred de una LAN conectada directamente. En una configuración típica, requiere la habilitación del direccionamiento de subred ARP de proxy, para permitir que el direccionador responda a peticiones ARP a sistemas principales en la red local, en nombre de los clientes de marcación de entrada.

Configuración básica de DHCP

La configuración más básica llama a un único servidor DHCP en la misma red que el direccionador, con direcciones de marcación de entrada que deben alquilarse en la misma subred que esta LAN.

Cuando el cliente realiza la marcación de entrada, se obtiene un alquiler para una dirección IP del servidor DHCP y se utiliza en la negociación de IPCP con el cliente.

1. Conecte 2216 y DHCP a la misma LAN.
2. Configure e inicie el servidor DHCP (consulte la documentación del servidor DHCP para saber cómo configurar el servidor para alquilar direcciones IP).

Recuerde que las direcciones IP que deben asignarse DEBEN estar dentro de una subred de una LAN conectada directamente y ARP de proxy debe estar habilitado en el 2216).

3. La configuración típica para Proxy DHCP inhabilita las opciones Client-Specified, Userid e Interface and Pool IP Address Negotiation:

```
Dials Config>list ip
DIALs client IP address specification:
Client : disabled
UserID : disabled
Interface : disabled
DHCP Proxy : enabled
```

4. Añada el servidor DHCP (Dials Config> **add dhcp 10.0.0.111**)
5. Defina el software de cliente de marcación de entrada como *Server assigned*.

Notas:

- a. La configuración de *Server assigned* varía entre distintas implementaciones de cliente de marcación de entrada.
 - b. El software de cliente no se debe configurar para obtener su dirección de DHCP. El cliente debe obtener su dirección enviando una dirección 0.0.0.0 a IPCP en la petición de configuración inicial.
6. Para esta configuración, deje que DHCP GATEWAY ADDRESS tome el valor por omisión 0.0.0.0.

Múltiples saltos al servidor DHCP

El servidor o servidores DHCP que se han configurado deben ser direcciones IP que se pueden alcanzar desde el direccionador conectado. Siempre debe poder hacer PING en el servidor desde el recuadro de acceso remoto.

Cuando el servidor DHCP está ubicado a varios saltos de distancia, el servidor tiene que conocer una dirección a la que responder, e indicar de qué agrupación se debe asignar una dirección IP. La agrupación de la que se asigna una dirección IP es importante, porque el servidor DHCP podría utilizarse para servir direcciones a un número de subredes y debe haber alguna indicación sobre la agrupación de direcciones de la que se debe seleccionar. Para esto se utiliza la Dirección de pasarela DHCP (*giaddr*) (la terminología se basa en la definición dada en el documento RFC 2131). *giaddr* debe ser una dirección que sea local para el 2216, como el puerto de LAN de Red en Anillo o Ethernet. Además, dado que *giaddr* es la dirección que el servidor DHCP utilizará para contestar, asegúrese de que puede realizar PING en esta dirección desde el mismo servidor DHCP.

Red de varios servidores DHCP

Puede configurar varios servidores DHCP como redundancia. Cuando configure varios servidores, el cliente de Proxy DHCP solicita una dirección a todos los servidores y acepta la primera respuesta recibida. Si cualquiera de los servidores DHCP está a más de un salto de distancia, o está conectado a una subred que no está asociada a las direcciones de su agrupación, es preciso configurar *giaddr*. Vea "Múltiples saltos al servidor DHCP".

Mientras pueda haber más de un servidor DHCP que ofrece direcciones, es importante no permitir que se solape la agrupación de direcciones configuradas en cada servidor. Además, dado que sólo hay un *giaddr* para que el servidor DHCP responda y realice una consulta, cada agrupación de direcciones debe estar en la misma subred que las otras.

Servidor de nombres de dominio dinámico (DDNS)

Un Servidor de nombres de dominio (DNS) correlaciona direcciones IP con los nombres de sistema principal y es normalmente de naturaleza estática. El DNS dinámico es una característica que, cuando se utiliza con un servidor DDNS DHCP y un servidor DNS, habilita DHCP para actualizar dinámicamente el servidor DNS con una correlación de direcciones IP y nombres de sistema principal. Esta característica sólo puede utilizarse junto con Proxy DHCP.

Cuando habilite DNS Dinámico en el 2216 y configure un nombre de sistema principal en el perfil de usuario (consulte “PPP Authentication Protocols” en el manual *Nways Multiprotocol Access Services Guía del usuario de software*), este nombre de sistema principal se pasa como la opción 81 (DDNS) al DHCP SERVER. Si ha configurado correctamente el servidor DHCP para DDNS, el servidor DHCP actualiza el servidor DDNS con la dirección IP que se alquila al direccionador y el nombre de sistema principal que envió el direccionador. Esto permite a otros usuarios acceder al cliente de marcación de entrada a través del nombre de sistema principal, en lugar de requerir que el cliente conozca la dirección IP elegida dinámicamente.

Configuración de DIAL

Este capítulo describe la configuración y los mandatos operativos de DIALs. Este capítulo incluye:

- “Acceso al entorno de configuración global de DIAL”
- “Mandatos de configuración global de DIAL”
- “Acceso al entorno de supervisión global de DIAL” en la página 503
- “Mandatos de supervisión global de DIAL” en la página 503

Acceso al entorno de configuración global de DIAL

Utilice el siguiente procedimiento para acceder al proceso de configuración global.

1. En el indicador OPCON, entre **talk 6**. (Para obtener más detalles sobre este mandato, consulte *The OPCON Process and Commands* en el manual Nways Multiprotocol Access Services Guía del usuario de software.) Por ejemplo:

```
* talk 6
Config>
```

Después de entrar el mandato **talk 6**, el indicador CONFIG (Config>) se visualiza en la terminal. Si el indicador no aparece al entrar la configuración por primera vez, pulse de nuevo **Return**.

2. En el indicador CONFIG, entre el mandato **feature dials** para acceder al indicador DIALs Config> y al entorno de configuración de parámetros globales de DIAL.

Mandatos de configuración global de DIAL

Tabla 60. Mandatos de configuración global de DIAL

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxiv.
Add	Añade un servidor DHCP (Dynamic Host Configuration Protocol) a la lista de servidores DHCP, o añade una agrupación de direcciones IP.
Delete	Suprime un servidor DHCP de la lista o elimina un bloque de direcciones de una agrupación de direcciones IP.
Disable	Inhabilita los métodos de asignación de direcciones IP, MP de multichasis, Mensajes de cabecera SPAP y DNS dinámico.
Enable	Habilita varios métodos de asignación de direcciones IP, MP de multichasis, Mensajes de cabecera SPAP y DNS dinámico.
List	Lista los parámetros de DIALs global y sus valores.
Set	Define el tiempo permitido, la dirección de pasarela DHCP, las direcciones de Servidor de nombres de NetBIOS, las direcciones MAC asignadas localmente, Conexiones virtuales (VC) y las direcciones de Servidor de nombres dinámico.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiv.

Add

Utilice el mandato **add** para añadir un nuevo servidor Proxy DHCP a una lista de servidores o para añadir una agrupación IP de direcciones.

La lista del servidor Proxy DHCP contiene las direcciones IP de los servidores DHCP que, a su vez, alquilarán las direcciones IP a los clientes de marcación de entrada. Pueden añadirse varios servidores como redundancia. El número máximo de servidores es 20.

La característica de agrupación de direcciones IP proporciona un método mediante el cual el direccionador puede recuperar una dirección IP de una agrupación de direcciones definida localmente en un cliente de marcación de entrada. El cliente puede utilizar esta dirección mientras dure la conexión con el direccionador. Una agrupación se compone de uno o más bloques de direcciones IP. El número máximo de bloques es 20. Cada uno de estos bloques se define mediante una dirección IP base y el número de direcciones en el bloque. Las direcciones de cada bloque son ascendentes y contiguas, empezando por la dirección base.

Sintaxis:

```
add                dhcp-server dirección-ip  
                    ip-pool dirección-base núm-direcciones
```

dhcp-server *dirección-ip*

Añade un servidor DHCP con la dirección IP especificada.

Ejemplo:

```
DIALs Config> add dhcp-server  
DIALs Proxy DHCP server address [0.0.0.0]? 10.0.0.1
```

ip-pool *dirección-base núm-direcciones*

Añade un bloque de direcciones a la agrupación IP.

Ejemplo:

```
DIALs Config> add ip-pool  
Base address []? 192.1.100.18  
Number of addresses [1]? 57  
DIALs config>add ip-pool  
Base address []? 192.2.200.1  
Number of addresses [1]? 250  
DIALs config>list ip-pools  
Configured IP address pools:  
Base Address      Last Address      Number  
-----  
192.1.100.18     192.1.100.74     57  
192.2.200.1      192.2.200.250    250
```

Delete

Utilice el mandato **delete** para suprimir un servidor existente de Proxy DHCP de la lista de servidores, o para eliminar un bloque de direcciones de la agrupación de direcciones IP.

Sintaxis:

```
delete            dhcp-server dirección-ip  
                    ip-pool dirección-base núm-direcciones
```

dhcp-server *dirección-ip*

Elimina un servidor DHCP con la dirección IP especificada.

Ejemplo:

```
DIALs Config> delete dhcp-server
Enter the address to be deleted [0.0.0.0]? 10.0.0.1
```

ip-pool *dirección-base núm-direcciones*

Elimina un bloque de direcciones de la agrupación IP.

Ejemplo:

```
DIALs Config> delete ip-pool
Base IP address of the block to be removed []? 192.2.200.1
```

Disable

Utilice el mandato **disable** para inhabilitar un método de asignación de direcciones IP, Mensajes de cabecera SPAP y DNS dinámico.

Sintaxis:

```
disable           dynamic-dns
                   ip-address-assignment tipo
                   spap-banner
```

dynamic-dns

Inhabilita el envío de la opción 81 de DHCP para el nombre de sistema principal del usuario. Consulte “Servidor de nombres de dominio dinámico (DDNS)” en la página 494 para obtener más información.

IP-address-assignment *type*

Inhabilita varias técnicas de asignación de direcciones IPCP. Puede especificar cualquiera de los siguientes:

- Cliente – Evita la asignación de direcciones IP asignadas por el cliente.
- ID de usuario – Evita la utilización del perfil de usuario autenticado para una dirección IP.
- Interfaz – Evita que el direccionador utilice los valores de IPCP para la interfaz.
- Agrupación – Evita que el direccionador utilice la agrupación de direcciones IP para asignar direcciones a clientes.
- DHCP Proxy – Evita que el direccionador alquile una dirección del servidor DHCP.

Consulte “Direcciones IP proporcionadas por el servidor” en la página 490 para obtener información adicional acerca de las técnicas de asignación.

spap-banner

Inhabilita el envío de un mensaje de cabecera SPAP a un usuario remoto autenticado con SPAP.

Nota: Entrar \n obligará a la inserción de un carácter de línea nueva en el mensaje de cabecera visualizado en el cliente.

Enable

Utilice el mandato **enable** para habilitar la asignación de direcciones IP, Mensajes de cabecera SPAP y DNS dinámico.

Sintaxis:

```
enable          dynamic-dns  
                  ip-address-assignment . . .  
                  spap-banner
```

dynamic-dns

Habilita el envío de la opción 81 de DHCP para el nombre de sistema principal del usuario. Consulte “Servidor de nombres de dominio dinámico (DDNS)” en la página 494 para obtener más información.

IP-address-assignment type

Habilita varias técnicas de asignación de direcciones IPCP. El direccionador intentará todos los métodos habilitados, en el orden en que aparecen en la lista. Puede especificar cualquiera de los siguientes:

- Cliente – Permite que el cliente especifique la dirección que desea utilizar.
- ID de usuario – El direccionador buscará una dirección IP en el perfil de usuario PPP autenticado. Si la dirección es distinta de cero, se ofrecerá al cliente.
- Interfaz – El direccionador consultará la dirección IP configurada en la interfaz. Si la dirección es distinta de cero, se ofrecerá al cliente.
- Agrupación – El direccionador solicitará una dirección de la agrupación de direcciones IP. Si la dirección está disponible, se ofrecerá al cliente.
- DHCP Proxy – El direccionador intentará alquilar una dirección de DHCP. Si la operación es satisfactoria, se ofrecerá la dirección al cliente.

Consulte “Direcciones IP proporcionadas por el servidor” en la página 490 para obtener información adicional acerca de las técnicas de asignación.

spap-banner

Habilita el envío de un mensaje de cabecera SPAP a un usuario remoto autenticado con SPAP. Utilice el mandato **set spap-banner** descrito en “Set” en la página 500 para entrar el texto del mensaje de cabecera SPAP. Consulte “Shiva Password Authentication Protocol (SPAP)” en el manual *Nways Multiprotocol Access Services Guía del usuario de software* para obtener más información.

List

Utilice el mandato **list** para visualizar la configuración actual. Se pueden supervisar el estado de DHCP y el tiempo de alquiler para cada red desde la consola Punto a punto. Consulte el mandato **listipcp** en el manual *Nways Multiprotocol Access Services Guía del usuario de software* para ver un ejemplo.

Sintaxis:

```
list          all
              dhcp-servers
              dynamic-dns
              ip-address-assignment
              ip-pools
              name-servers
              spap-banner
              time-allowed
              vc-parameters
```

Ejemplo:

```
DIALs config>li all
DIALs client IP address assignment:
Client      : Enabled
UserID     : Enabled
Interface  : Enabled
Pool       : Enabled
DHCP Proxy : Disabled

Configured IP address pools:
  Base Address   Last Address   Number
  -----
  11.0.0.100     11.0.0.129     30
  11.0.0.210     11.0.0.229     20

Configured DHCP servers:          11.0.0.2          11.0.0.50
Proxy DHCP is currently disabled
DHCP gateway address (giaddr): 11.0.0.10

Dynamic DNS: Enabled

Primary Domain Name Server (DNS): 11.0.0.2
Secondary Domain Name Server (DNS): None
Primary NetBIOS Name Server (NBNS): 11.0.0.2
Secondary NetBIOS Name Server (NBNS): None

Time allowed for connections: Unlimited

SPAP banner :Enabled
Welcome to the network...

Number of Mac Addresses defined = 0
Base MAC Address: 000000000000

VC: Maximum Virtual Connections = 50
VC: Maximum suspend time (hours) (0 is unlimited) = 12
VC: Idle timeout period (seconds) = 30

Multi-chassis MP: Endpoint discriminator (0 means use box s/n) = 0

DIALs config>
```

El ejemplo muestra lo siguiente:

DIALs client IP address specification

Visualiza las técnicas de asignación de direcciones IP y si están habilitadas o no. Recibirá esta sección de la visualización como respuesta al mandato **list ip-address-assignment**.

Configuración de DIALs

IP address pools

Visualiza las agrupaciones de direcciones IP configuradas. Recibirá esta sección de la visualización como respuesta al mandato **list ip-pool**.

Configured DHCP servers

Visualiza la lista de direcciones IP configuradas actualmente como servidores DHCP. Esta sección lista también la interfaz que se utiliza para la pasarela DHCP. Recibirá esta sección de la visualización como respuesta al mandato **list dhcp-servers**.

Dynamic Name Servers

Visualiza si el DNS dinámico está habilitado o no. Recibirá esta sección de la visualización como respuesta al mandato **list dynamic-dns**.

primary domain server (dns)

Esta línea y las siguientes visualizan los servidores de nombres primario y secundario. Recibirá esta sección de la visualización como respuesta al mandato **list name-servers**.

time allowed

Visualiza la cantidad máxima de tiempo (en minutos) para los usuarios de marcación. Recibirá esta sección de la visualización como respuesta al mandato **list time-allowed**.

spap banner

Visualiza el contenido del mensaje de cabecera SPAP. Recibirá esta sección de la visualización como respuesta al mandato **list spap-banner**.

vc connections

Visualiza información acerca de las conexiones virtuales configuradas.

multi-chassis mp

Visualiza el discriminador de extremo configurado.

Set

Utilice el mandato **set** para definir el tiempo permitido, la dirección de pasarela DHCP, las direcciones de Servidores de nombres de NetBIOS, las direcciones de Servidores de nombres dinámicos.

Sintaxis:

```
set          dhcp-gateway-address  
              dns . . .  
              laa  
              multi-chassis-mp  
              nbns . . .  
              spap-banner . . .  
              time-allowed  
              vc-parameters
```

dhcp-gateway-address *núm-interfaz dirección-ip*

Define la dirección IP asociada a la pasarela DHCP. DHCP utiliza la dirección como:

1. Una dirección a la que contesta DHCP

- Una indicación de la agrupación de direcciones desde la que DHCP asigna una dirección IP

Si el servidor DHCP no está en una interfaz de LAN conectada directamente, debe configurar esta dirección como la dirección de una de las interfaces de LAN que tiene conectividad IP con el servidor DHCP. Consulte “DHCP (Dynamic Host Configuration Protocol)” en la página 492 y la definición de “giaddr” en el documento RFC 1541 para obtener más información.

dns tipo dirección-ip

Configura los servidores de nombres de dominio primario y secundario (DNS). **Tipo** puede ser:

primary

Define la dirección IP del servidor DNS primario para que la utilice el cliente de marcación de entrada. Este valor se negocia durante IPCP para algunos clientes de marcación (en especial, los de Windows 95).

secondary

Define la dirección IP del servidor DNS secundario para que la utilice el cliente de marcación de entrada. Este valor se negocia durante IPCP para algunos clientes de marcación (en especial, los de Windows 95).

laa núm_direcciones_MAC dirección_MAC_base

Define el número de MAC y la dirección base para la tabla de LAA (Dirección administrada localmente). Sólo las redes Layer-2-Tunneling utilizan direcciones LAA.

núm_direcciones_MAC

Especifica el número de direcciones MAC que deben añadirse a la tabla de LAA, empezando por *dirección_MAC_base*.

Valores válidos: 0 a 256

Valor por omisión: 0

dirección_MAC_base

Especifica la dirección MAC de la tabla de LAA.

Valores válidos: cualquier dirección MAC válida

Valor por omisión: 000000000000

Ejemplo:

```
DIALs config>set laa
Number of Mac Addresses: [0]? 20
Locally Administered Mac Address Base (hex) [000000000000]? 00210aaaaa
DIALs Config>
```

multi-chassis-mp

Define el discriminador de extremo que debe utilizarse. Todos los enlaces que deben unir el mismo paquete deben tener el mismo discriminador de extremo.

Ejemplo:

```
DIALs Config> set multi-chassis-mp
Enter Endpoint Discriminator to use from stacked group (0 for box S/N): 2345
```

nbns *tipo dirección-ip*

Configura los servidores de nombres NetBIOS primario y secundario.

Tipo puede ser:

primary Define la dirección IP del servidor de nombres NetBIOS primario.

secondary

Define la dirección IP del servidor de nombres NetBIOS secundario.

spap-banner

Permite la configuración de un mensaje que se envía a todos los clientes que completan satisfactoriamente la autenticación SPAP.

Ejemplo:

```
DIALs config>set spap-banner
SPAP banner :Disabled
```

```
Enter Banner: Welcome to the network...
```

time-allowed

Define el tiempo permitido a los usuarios de marcación de entrada. Este parámetro define la cantidad máxima de tiempo (en minutos) que puede estar conectado un usuario. El valor por omisión es 0, lo que quiere decir que el usuario puede estar conectado durante un período de tiempo ilimitado.

vc-parameters

Utilice este parámetro para definir los atributos globales de conexión virtual por omisión. El sistema le solicitará el número máximo de conexiones, el tiempo máximo de suspensión y el valor de tiempo de espera de inactividad.

Ejemplo:

```
Config> feature DIALs
DIALs Config> set vc-parameters
Maximum Virtual Connections [50]? 40
Maximum suspended time (hours) (0 is unlimited) [10]? 18
Inactivity Timeout (seconds) [30]? 60
DIALs Config>
```

Maximum Virtual Connections Número máximo de conexiones virtuales (VC) que pueden estar activas o suspendidas. Al utilizar VC con MP, configure este valor para que sea 1 mayor que el número de conexiones físicas.

Valores válidos: 0 a 255

Valor por omisión: 50

Maximum suspended time Cantidad máxima de tiempo, en horas, que puede suspenderse una conexión virtual antes de que el sistema finalice la conexión. Especificar 0 para este parámetro permite que una conexión virtual se suspenda indefinidamente.

Valores válidos: 0 a 48

Valor por omisión: 12

Tiempo de espera de inactividad Número de segundos que una conexión virtual puede estar inactiva antes de suspenderse.

Valores válidos: 10 a 1024

Valor por omisión: 30

Acceso al entorno de supervisión global de DIAL

Utilice el siguiente procedimiento para acceder a los mandatos de supervisión de DIALs.

1. En el indicador OPCON, entre **talk 5**. (Para obtener detalles acerca de este mandato, consulte el capítulo “The OPCON Process and Commands” del manual *Nways Multiprotocol Access Services Guía del usuario de software*.)
Por ejemplo:

```
* talk 5
+
```

Después de entrar el mandato **talk 5**, el indicador GWCON (+) se visualiza en la terminal. Si el indicador no aparece al entrar la configuración por primera vez, pulse de nuevo **Return**.

2. En el indicador +, entre el mandato **feature dials** para acceder al indicador DIALS Console> y al entorno de supervisión global.

Ejemplo:

```
+ feature dials
DIALS Console>
```

Mandatos de supervisión global de DIAL

Tabla 61. Mandatos de supervisión global de DIAL

Mandato	Función
Clear	Borra una conexión virtual suspendida específica.
List	Visualiza el estado de diversas conexiones virtuales o de todas ellas.
Reset	Activa dinámicamente los parámetros de DIALs.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiv.

Clear

Utilice el mandato **clear** para borrar conexiones virtuales suspendidas específicas.

Sintaxis:

```
clear          vc connection_id
```

vc connection_id Especifica la conexión virtual suspendida que finaliza. Para obtener el valor de *connection_id*, entre el mandato **list all-vc** o **list suspended-vcs**.

List

Utilice el mandato **list** para visualizar los valores de los parámetros de VC o todas las conexiones virtuales, activarlas y suspenderlas.

Sintaxis:

```
list          all
              active-vcs
              all-vcs
              dhcp-servers
              ip-address-assignment
              ip-pool
              suspended-vcs
```

active-vcs Visualiza los atributos de todas las conexiones virtuales activas. Vea la descripción del parámetro **all-vcs** para obtener una explicación de los atributos.

all-vcs Visualiza los atributos de todas las conexiones virtuales activas y suspendidas. Esta pantalla es una combinación de las pantallas de los mandatos **list active-vcs** y **list suspended-vcs**.

Ejemplo:

```
+ feature dials
DIALS console> list all
DIALs client IP address assignment:
Client      : Enabled
UserID      : Enabled
Interface   : Enabled
Pool        : Enabled
DHCP Proxy  : Disabled

Current IP address pools:
      Base Address      Last Address      Total      Free
      -----
*    11.0.0.100        11.0.0.129        30         30
      11.0.0.210        11.0.0.229        20         19

Current DHCP servers:          11.0.0.2          11.0.0.50
Proxy DHCP is currently disabled
DHCP gateway address (giaddr): 11.0.0.10

Active VCs:
Conn ID   Interface Idle-Timeout Connected Username
=====   =====
1656494850      8      30      0:26:15 don
7293521502      9      30      1:41:57 jane

Suspended VCs:
              Hrs.Max
Conn ID   Suspend Suspended Username
=====   =====
9256166098      12      0: 4:13 joe
```

Los atributos de las VC activas y suspendidas son los siguientes:

Conn ID El ID de conexión de la conexión virtual. El sistema asigna el ID al establecer la conexión.

Username El usuario AAA. RADIUS o usuario de lista local que establece la conexión virtual.

Para las VC activas:

Interface Interfaz de red que gestiona la conexión virtual.

Nota: No asigne direcciones IP a clientes de marcación utilizando la asignación de interfaz para evitar problemas causados por otros usuarios que utilicen esta interfaz con la VC suspendida.

Idle Timeout Cantidad de tiempo, en segundos, tras la cual el sistema suspenderá la VC. Esto corresponde al valor del temporizador de inactividad en el mandato **set**.

Connected HHH:MM:SS Cantidad de tiempo total, en horas, minutos y segundos, que la VC ha estado conectada a una interfaz.

Para las VC suspendidas:

Hrs. Max Suspended Número máximo de horas que una VC puede estar en estado suspendido antes de que el sistema finalice la conexión. Esto corresponde al valor del tiempo máximo de suspensión en el mandato **set**.

Suspended HH:MM:SS Cantidad de tiempo total, en horas, minutos y segundos, que la VC ha estado suspendida.

dhcp-servers Visualiza la información configurada acerca de los servidores DHCP y sus direcciones IP.

ip-address-assignment Visualiza los métodos mediante los cuales se pueden asignar direcciones IP a clientes

ip-pool Visualiza la utilización actual de la agrupación.

Ejemplo:

```
DIALs Console> list ip-pool
```

```
Current IP address pools:
```

	Base Address	Last Address	Total	Free
*	192.1.100.18	192.1.100.74	57	57
	192.2.200.1	192.2.200.250	250	250

Nota: El * indica de qué bloque se recuperará la siguiente dirección.

suspended-vcs Visualiza los atributos de todas las conexiones virtuales suspendidas. Vea la descripción del parámetro **all-vcs** para obtener una explicación de los atributos.

vc-parameters Visualiza los valores de los parámetros de VC que se han definido mediante el mandato **set vc-parameters**.

Reset

Utilice el mandato **reset** para activar dinámicamente los cambios en la configuración realizados en la interfaz DIALs en talk 6.

Sintaxis:

```
reset all
```

Configuración de DIALs

dhcp-parameters

ip-address-assignment

ip-pool

vc-parameters

all Activa dinámicamente los cambios de DHCP, asignación de direcciones IP y configuración de agrupación IP.

dhcp-parameters

Activa dinámicamente la configuración de DHCP.

ip-address-assignment

Activa dinámicamente la configuración del método de asignación de direcciones IP.

ip-pool Activa dinámicamente la configuración de la agrupación de direcciones IP.

vc-parameters

Actualiza dinámicamente los cambios de configuración de VC.

Utilización del servidor DHCP

Este capítulo describe cómo utilizar el servidor DHCP. Incluye las secciones siguientes:

- “Introducción a DHCP”
- “Conceptos y terminología” en la página 512
- “Servidor DHCP y parámetros de alquiler” en la página 515
- “Opciones de DHCP” en la página 515
- “Configuración de IP para DHCP” en la página 529
- “Configuración de ejemplo de servidor DHCP” en la página 530

Introducción a DHCP

DHCP (Dynamic Host Configuration Protocol) es un protocolo cliente/servidor basado en el protocolo BOOTP (Bootstrap Protocol). El servidor DHCP proporciona direcciones IP reutilizables, controladas de manera centralizada, y otras informaciones de configuración de TCP/IP para los clientes DHCP. Su funcionalidad puede aliviar el peso que soportan los Network Managers al distribuir la información de configuración a los usuarios nuevos y ya existentes. Esta característica es conforme al documento RFC 2131, aunque da soporte a muchas características adicionales que no están incluidas en este documento. También se da soporte a los clientes BOOTP, tal como está definido en el documento RFC 951.

Con DHCP, los clientes a los que se da soporte pueden difundir mensajes DISCOVER para encontrar servidores DHCP en su red y, posteriormente, recibir mediante OFFER sus datos de configuración de forma dinámica a través de la red. DHCP utiliza los puertos UDP BOOTP, conocidos públicamente (68 para el servidor y 67 para el cliente) para comunicar sus peticiones y respuestas. Los clientes y los servidores DHCP pueden utilizar agentes de BOOTP Relay existentes para ampliar su rango de servicio. DHCP ofrece muchas ventajas sobre las redes configuradas de forma estática, incluida la capacidad de dar soporte a redes que sufren modificaciones. A los clientes sólo se les alquila la dirección IP, de manera que, cuando el cliente ya no la necesite o se traslade a otra subred, la dirección se podrá liberar y dejarla disponible para que la utilice otro cliente.

Operación de DHCP

DHCP permite que los clientes obtengan información de configuración de la red IP, incluida una dirección IP, de un servidor DHCP central. Los servidores DHCP controlan si las direcciones que proporcionan a los clientes se asignan de forma permanente o se alquilan durante un período específico de tiempo. Cuando un cliente recibe una dirección alquilada, debe solicitar periódicamente que el servidor vuelva a validar la dirección y renueve el alquiler.

Los procesos de asignación de direcciones, alquiler y su renovación, son gestionados por los programas de cliente y servidor DHCP y son transparentes para los usuarios finales. Los clientes utilizan mensajes de arquitectura RFC para aceptar y utilizar las opciones que les sirve el servidor DHCP. Por ejemplo:

Utilización del servidor DHCP

1. El cliente difunde un mensaje (que contiene su ID de cliente) en el que anuncia su presencia y solicita una dirección IP (mensaje DHCPDISCOVER) y las opciones deseadas, como la máscara de subred, el servidor de nombres de dominio, el nombre de dominio y la ruta estática.
2. Opcionalmente, si los direccionadores de la red están configurados para reenviar mensajes DHCP y BOOTP (utilizando BOOTP Relay), el mensaje de difusión se reenvía a los servidores DHCP en las redes conectadas.
3. Cada servidor DHCP que recibe el mensaje DHCPDISCOVER del cliente envía un mensaje DHCPOFFER al cliente, ofreciendo una dirección IP. El servidor DHCP comprueba si hay direcciones IP duplicadas en la red antes de emitir una oferta. El servidor comprueba el archivo de configuración para ver si debe asignar al cliente una dirección estática o dinámica. En caso de que ofrezca una dirección dinámica, el servidor selecciona una dirección de la agrupación de direcciones, eligiendo la que se haya utilizado en la fecha menos reciente. Una agrupación de direcciones es un rango de direcciones IP que van a alquilarse a los clientes. En caso de que ofrezca una dirección estática, el servidor utiliza una sentencia de Cliente de la configuración del servidor DHCP para asignar las opciones a los clientes. Al realizar la oferta, el servidor DHCP reserva la dirección ofrecida.
4. El cliente recibe el mensaje o mensajes de oferta y selecciona el servidor que desea utilizar. Cuando un cliente DHCP recibe una oferta, toma nota de cuántas opciones, entre las solicitadas, se han incluido en la oferta. El cliente DHCP continúa recibiendo ofertas de los servidores DHCP para un período de 4 segundos después de haber recibido la primera oferta, tomando nota de cuántas de las opciones solicitadas están incluidas en cada oferta. Al finalizar este período de tiempo, el cliente DHCP compara todas las ofertas y selecciona la que cumple sus criterios.
5. El cliente difunde un mensaje para indicar el servidor que ha seleccionado y solicita el uso de la dirección IP ofrecida por ese servidor (mensaje DHCPREQUEST).
6. Si un servidor recibe un mensaje DHCPREQUEST que indica que el cliente ha aceptado la oferta del servidor, marcará esa dirección como alquilada. Si el servidor recibe un mensaje DHCPREQUEST que indica que el cliente ha aceptado una oferta de un servidor diferente, devolverá la dirección a la agrupación disponible. Si no se recibe ningún mensaje en un período de tiempo especificado, el servidor devolverá la dirección a la agrupación disponible. El servidor seleccionado envía al cliente un acuse de recibo que contiene información adicional sobre la configuración (mensaje DHCPACK).
7. El cliente determina si la información sobre la configuración es válida. Al recibir un mensaje DHCPACK, el cliente DHCP envía una petición de protocolo ARP (Address Resolution Protocol) a la dirección IP suministrada para ver si ya se está utilizando. Si recibe una respuesta a la petición ARP, el cliente declinará la oferta (mensaje DHCPDECLINE) e iniciará de nuevo el proceso. De lo contrario, el cliente aceptará la información sobre configuración.
8. Al aceptar un alquiler válido, el cliente entra un estado BINDING con el servidor DHCP y pasa a utilizar la dirección IP y las opciones. Si el cliente DHCP es un cliente de Dirección dinámica, el cliente DHCP notifica el Servidor de nombres de dominio dinámico de su correlación de direcciones de nombres a IP del sistema principal.

A los clientes DHCP que solicitan opciones, el servidor DHCP normalmente les proporciona opciones que incluyen la máscara de subred, el servidor de nombres de dominio, el nombre de dominio, la ruta estática, el identificador de clase (que indica un proveedor específico) y la clase de usuario.

Sin embargo, el cliente DHCP puede solicitar un conjunto de opciones propias y exclusivas. Por ejemplo, es necesario que los clientes DHCP de Windows NT 3.5.1 soliciten las opciones. El conjunto por omisión de opciones DHCP solicitado por el cliente y proporcionado por IBM, incluye la máscara de subred, el servidor de nombres de dominio, el nombre de dominio y la ruta estática. Vea las descripciones de las opciones en “Opciones de DHCP” en la página 515.

Renovación de alquileres

El cliente DHCP hace un seguimiento del tiempo de alquiler restante. En un momento determinado antes de la caducidad del alquiler, normalmente cuando ha transcurrido la mitad del plazo, el cliente envía al servidor que ofrece el alquiler una petición de renovación, que contiene su dirección IP actual y la información sobre configuración. Si el servidor responde con una oferta de alquiler, el alquiler del cliente DHCP queda renovado.

Si el servidor DHCP rechaza la petición de manera explícita, el cliente DHCP puede seguir utilizando la dirección IP hasta que caduca el período de alquiler y se inicia el proceso de petición de direcciones, incluida la difusión de dicha petición. Si no puede ponerse en contacto con el servidor, el cliente puede seguir utilizando la dirección asignada hasta que caduque el período de alquiler.

Movimiento de clientes

Una ventaja de DHCP es la libertad que proporciona a un sistema principal de clientes para moverse de una subred a otra, sin tener que saber por anticipado la información de configuración de IP que necesitará en la nueva subred. Mientras las subredes en las que un sistema principal se reubica tengan acceso a un servidor DHCP, un cliente DHCP se configurará automáticamente de manera correcta para acceder a esas subredes.

Para que los clientes DHCP vuelvan a configurar el acceso a una nueva subred, se debe reorganizar el sistema principal cliente. Cuando un sistema principal se reinicia en una nueva subred, el cliente DHCP intenta renovar su antiguo alquiler con el servidor DHCP que asignó la dirección originalmente. El servidor rehúsa renovar la petición, ya que la dirección no es válida en la nueva subred. Cuando no reciba ninguna respuesta del servidor ni instrucciones del servidor DHCP, el cliente iniciará el proceso de petición de dirección IP para obtener una nueva dirección IP y acceder a la red.

Modificación de las opciones del servidor

Con DHCP, puede efectuar cambios en el servidor, inicializar el servidor y distribuir las modificaciones entre todos los clientes adecuados. Un cliente DHCP retiene los valores de las opciones DHCP asignadas por el servidor DHCP mientras dure el alquiler. Si implementa cambios en la configuración en el servidor mientras un cliente se está ejecutando, el cliente no procesa estas modificaciones hasta que el cliente intenta renovar el alquiler o hasta que se reinicia.

Utilización del servidor DHCP

Nota: Si el servidor se vuelve a inicializar (utilizando el mandato `t 5reset dhcp`), se perderá la información del período de alquiler visualizada por el direccionador, hasta que los clientes DHCP renueven el alquiler.

Número de servidores DHCP

El número de servidores que necesitará, dependerá en gran medida del número de subredes que tenga, el número de clientes DHCP a los que piense dar soporte, si utilizará BOOTP Relay y el tiempo de alquiler que elija. Tenga en cuenta que actualmente el protocolo DHCP no define la comunicación de servidor a servidor. Por lo tanto, éstos no podrán compartir información, ni un servidor DHCP podrá trabajar como “copia de seguridad dinámica” en caso de que el otro sufra una anomalía. Los clientes DHCP envían mensajes de difusión general. Por razones del diseño, los mensajes de difusión no cruzan subredes. Para permitir que se reenvíen los mensajes del cliente fuera de su subred, es preciso configurar direccionadores adicionales para reenviar peticiones DHCP utilizando el agente BOOTP Relay. De lo contrario, tendrá que configurar un servidor DHCP en cada subred.

Un único servidor DHCP

Si elige utilizar un único servidor DHCP para servir a sistemas principales en una subred, piense en los efectos que se producirán si falla el único servidor. Por lo general, una anomalía en un servidor afecta sólo a los clientes DHCP que intentan unirse a la red. Normalmente, el funcionamiento de los clientes DHCP que ya están en la red no se ve afectado hasta la caducidad del alquiler. No obstante, los clientes con un tiempo de alquiler corto pueden perder el acceso a la red antes de que se pueda reiniciar el servidor. Para minimizar el impacto de desconexión del servidor si sólo tiene un servidor DHCP para una subred, debe elegir un tiempo de alquiler lo bastante largo para reiniciar o responder al servidor DHCP anómalo.

Múltiples servidores DHCP

Para evitar un único punto de anomalía, puede configurar dos o más DHCP para que sirvan a la misma subred. Si un servidor falla, el otro puede continuar sirviendo a la subred. Cada uno de los servidores DHCP debe ser accesible mediante la conexión directa a la subred o mediante un agente BOOTP Relay.

Dado que dos servidores DHCP no pueden servir las mismas direcciones, las agrupaciones de direcciones definidas para una subred deben ser exclusivas entre los servidores DHCP. Por consiguiente, cuando utilice dos o más servidores DHCP para que sirvan una subred específica, será preciso dividir la lista completa de direcciones para esa subred entre los servidores. Por ejemplo, puede configurar un servidor con una agrupación de direcciones que consista en el 70% de las direcciones disponibles para la subred y otro servidor con una agrupación de direcciones que consista en el 30% restante de las direcciones disponibles.

La utilización de varios servidores DHCP reduce la probabilidad de tener una anomalía de acceso a red relativa a DHCP, pero no es ninguna garantía. Si falla un servidor DHCP para una subred específica, es posible que el otro servidor DHCP no pueda dar servicio a todas las peticiones de los nuevos clientes que, por ejemplo, podrían agotar la limitada agrupación de direcciones disponibles del servidor.

No obstante, puede favorecer que un servidor DHCP agote antes su agrupación de direcciones. Los clientes DHCP tienden a seleccionar el servidor DHCP que ofrece más opciones. Para favorecer el servicio hacia el servidor DHCP que tiene el 70% de las direcciones disponibles, ofrezca menos opciones de DHCP del otro servidor, que contiene el 30% restante de las direcciones disponibles para la subred.

Servidores BOOTP

Si ya tiene clientes y servidores BOOTP en la red, tal vez desee tomar en consideración la sustitución de los servidores BOOTP con servidores DHCP. Opcionalmente, los servidores DHCP pueden servir a los clientes BOOTP la misma información de configuración de IP que los servidores BOOTP actuales. Si no puede sustituir los servidores BOOTP con servidores DHCP y desea que ambos sirvan a su red, se recomienda tomar las siguientes precauciones:

- Desactive el soporte de BOOTP en el servidor DHCP.
- Asegúrese de que los servidores BOOTP y DHCP no conceden las mismas direcciones.
- Configure el soporte de BOOTP Relay en los direccionadores para reenviar difusiones de BOOTP a los servidores BOOTP y DHCP adecuados.

Un servidor DHCP asigna una dirección IP permanente a un cliente BOOTP. En caso de que las subredes se reenumeren de tal manera que una dirección asignada por BOOTP no sea utilizable, el cliente BOOTP debe reiniciarse y obtener una nueva dirección IP.

Clientes DHCP especiales

Puede tener clientes DHCP o Network Servers que tengan necesidades administrativas individuales o especiales, tales como:

- Alquiler permanente:

Puede asignar alquileres permanentes a los sistemas principales designados, especificando un tiempo de alquiler infinito. Además, el servidor DHCP asignará un alquiler permanente a los clientes BOOTP que lo soliciten de manera explícita, mientras esté habilitado el soporte de clientes BOOTP. El servidor DHCP también asignará un alquiler permanente a los sistemas principales DHCP que lo soliciten de forma explícita.
- Dirección IP específica:

Puede reservar una dirección específica y los parámetros de configuración para un sistema principal cliente DHCP o BOOTP específico en una subred determinada.
- Parámetros de configuración específica:

Puede asignar información de configuración específica a un cliente, sea cual sea su subred.
- Estaciones de trabajo definidas manualmente:

Debe excluir explícitamente las direcciones de las subredes DHCP para los sistemas principales existentes que no utilizan DHCP o BOOTP para configurar su acceso de red IP. Aunque los servidores y clientes DHCP comprueban automáticamente si una dirección IP se está utilizando antes de asignarla o utilizarla, no podrán detectar las direcciones de sistemas principales definidos manualmente que se desconectan de la red de manera total o temporal. En

este caso, pueden producirse problemas de direcciones duplicadas cuando un sistema principal definido manualmente vuelve a acceder a la red, a menos que se excluya explícitamente su dirección IP.

Períodos de tiempo de alquiler

El período de tiempo de alquiler por omisión es de 24 horas. Tenga en cuenta que el período de tiempo de alquiler de DHCP puede afectar a la operación y al rendimiento de la red:

- Unos períodos de alquiler cortos aumentarán la cantidad de tráfico de red, debido a unas peticiones de renovación de alquiler de DHCP. Por ejemplo, si define un período de alquiler de 5 minutos, cada cliente enviará una petición de renovación cada 2,5 minutos aproximadamente.
- Los períodos de alquiler demasiado largos pueden limitar la capacidad de volver a utilizar las direcciones IP. Períodos de alquiler muy prolongados también retardan los cambios de configuración que se producen cuando un cliente se reinicia o renueva un alquiler.

El período de alquiler que elija dependerá en gran medida de sus necesidades, incluyendo:

- El número de sistemas principales a los que se da soporte, comparado con el número de direcciones disponibles. Si tiene más sistemas principales que direcciones, tal vez desee elegir un período de alquiler breve, de una o dos horas. Esto ayudará a asegurar que las direcciones no utilizadas se devuelvan a la agrupación lo antes posible.
- El tiempo disponible para realizar cambios en la red. Los sistemas principales reciben cambios en la información de configuración cuando se reinician o renuevan el alquiler. Asegúrese de permitir que haya una ventana oportuna y adecuada para realizar estos cambios. Por ejemplo, si suele realizar los cambios por la noche, puede asignar un período de alquiler de 12 horas.
- El número de servidores DHCP que están disponibles. Si sólo tiene unos pocos servidores DHCP para una red grande, tal vez desee seleccionar un período de alquiler más largo para minimizar la influencia del tiempo de desconexión del servidor.

En el caso de las redes complejas, que tienen que dar soporte a una combinación de requisitos de alquiler de sistema principal, puede definir clases DHCP.

Conceptos y terminología

Los siguientes conceptos se utilizan para describir la función de servidor DHCP:

Scope El término "ámbito" (scope), al analizar la configuración del servidor DHCP, se utilizará para identificar a qué pertenece un determinado parámetro. La Figura 45 en la página 513 ilustra los ámbitos siguientes:

- Opción global 1
- Opción global 3
- Clase global ClaseA

ClaseA ha redefinido la opción 1, pero heredará el valor de la opción 3 del ámbito global.

- Cliente global ClienteA

ClienteA ha redefinido la opción 3, pero heredará el valor de la opción 1 del ámbito global.

- subred SubA

- Redefine la Opción 1.
- Hereda el valor de la Opción 3 del ámbito global.
- Define ClaseA en el ámbito de SubA.

Redefine el valor de la opción 1, pero heredará el valor de la opción 3 de SubA (que también se hereda del ámbito global).

- Define ClienteB en el ámbito de SubA.

ClienteB ha redefinido la opción 3, pero heredará el valor de la opción 1 de SubA.

- opción de proveedor proveedorA

Las opciones de proveedor son excepciones. Son independientes y no se heredan fuera del ámbito de la propia opción de proveedor.

Ámbito global:

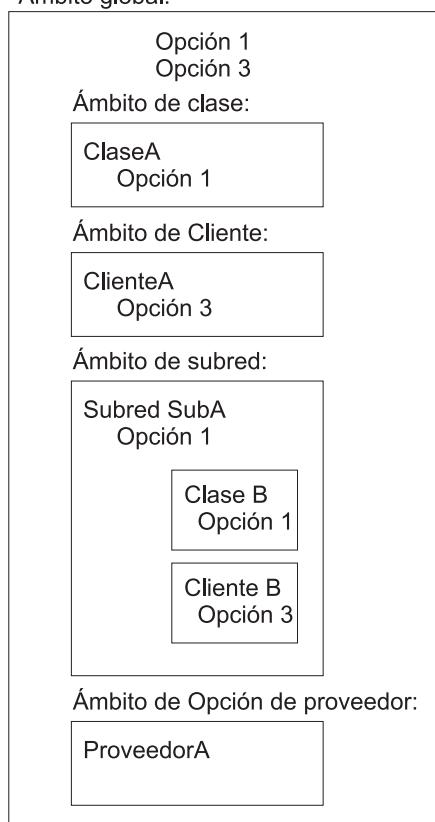


Figura 45. Conceptos sobre el ámbito

Subred Una subred define los parámetros de una agrupación de direcciones administrada por un servidor DHCP. Una agrupación de direcciones es un rango de direcciones IP que van a alquilarse a los clientes. Los parámetros que pueden especificarse incluyen el período de alquiler y otras opciones para los clientes que utilicen la agrupación de direcciones. El

período de alquiler y otras opciones pueden heredarse del ámbito global.

Grupos de subredes

Un grupo de subredes es una manera de identificar varias subredes que deben agruparse en la misma interfaz. A todas las subredes en un grupo determinado se les proporciona el mismo nombre de grupo de subredes y una prioridad exclusiva. La prioridad se utiliza para determinar el orden en que se entregarán las direcciones, según la política de direcciones con la que está asociado el grupo. Una subred puede pertenecer a una de dos políticas de direcciones:

- Inorder

Esta política es la que se toma por omisión. La política inorder administra direcciones, empezando por la subred que tiene la prioridad más baja y terminando por la subred con la prioridad más alta.

- Balance

La política balance administra las direcciones del grupo de subredes definidas por orden rotatorio. Se administra la primera dirección de la subred que tiene la prioridad más baja. Se administra la segunda dirección de la subred que tiene la siguiente prioridad más baja, y así sucesivamente. Cuando se haya administrado una dirección de la subred de prioridad más alta, la política regresará a la subred que tiene la prioridad más baja, hasta que se agoten todas las direcciones de todas las subredes del grupo.

Clases Una clase define los parámetros para un grupo de clientes definido por el usuario y administrado por el servidor DHCP. Pueden definirse las clases bajo un ámbito global o de subred. Cuando se define una clase en un ámbito de subred, el servidor DHCP sólo servirá a los clientes de la clase que estén ubicados en la subred especificada y soliciten la clase. Sólo las clases que se definan en el ámbito de una subred pueden especificar un rango de direcciones. El rango puede ser un subconjunto del rango de subred, o puede ser igual que el rango de subred. Si está disponible, se ofrece una dirección IP del rango de subred a un cliente que solicite una dirección IP de una clase que haya agotado su rango. Al cliente se le ofrecen las opciones asociadas a la clase agotada.

Clientes Un cliente puede utilizarse para:

- Definir una dirección IP estática y opciones de DHCP para una estación final específica
- Excluir del servicio una estación final específica
- Excluir una dirección IP de un rango de direcciones IP disponibles

Cada cliente tiene un tipo de hardware, un ID de cliente y una dirección IP determinados. Los tipos de hardware están definidos en el documento RFC 1340 y se muestran a continuación. Para todos los tipos de hardware además de 0, el ID de cliente es la dirección de hardware de la estación final (o dirección MAC). Para el tipo de hardware 0, el ID de cliente es una serie de caracteres. Normalmente, se trataría de un nombre de dominio.

Al definir un cliente, se le solicitará una dirección IP cualquiera (*any*) o ninguna (*none*). Si define una dirección IP, ésta se reservará para ese cliente. Si elige *any*, a ese cliente se le dará cualquier dirección IP disponible en esa subred. Si ha definido varios registros de subred en la misma subred, cada uno de ellos con un rango exclusivo, un cliente configurado con *any* obtendrá la primera dirección disponible en la subred, no necesariamente del rango del registro de subred específico en el que está definido el cliente. Si elige *none*, ninguna dirección IP servirá a esa estación final. Para excluir una dirección IP de su administración, debe definir un registro de cliente con un tipo de hardware y el ID de cliente 0.

Los tipos de hardware definidos por el documento RFC1340 y que pertenecen al IBM 2216 son:

Tipo de hardware	Valor
-----	-----
Reservado	0
Ethernet	1
Redes IEEE 802 (incluida Red en Anillo)	6

Para ver la lista completa, consulte el documento RFC 1340.

Servidor DHCP y parámetros de alquiler

Los siguientes parámetros de servidor DHCP pueden definirse a nivel global:

- bootstrapserver
- canonical
- lease expire interval
- lease time default
- ping time
- support unlisted clients
- support bootp
- used ip address expire interval

Consulte "Set" en la página 563 para ver una descripción de estos parámetros.

Opciones de DHCP

DHCP le permite especificar opciones para proporcionar información de configuración adicional a un cliente. Las opciones se definen en el documento RFC 2132 y otras RFC.

Formatos de opción

Todas las opciones esperan que los datos de configuración estén en uno de los formatos siguientes:

Formato	Definición
Dirección IP	Una única dirección IP en notación decimal con puntos.

Utilización del servidor DHCP

Direcciones IP	Una o más direcciones IP en notación decimal con puntos, separadas por blancos.
Par de direcciones IP	Dos direcciones IP en notación decimal con puntos, separadas por blancos.
Pares de direcciones IP	Uno o más pares de direcciones IP, cada par separado del siguiente por un blanco.
Booleano	0 ó 1 (Verdadero o Falso).
Byte	Número decimal entre -128 y 127 (inclusive).
Byte sin signo	Número decimal entre 0 y 255 (inclusive). No puede especificar un valor negativo para un byte sin signo.
Lista de bytes sin signo	Uno o más números decimales entre 0 y 255 (inclusive), separados por blancos. No puede especificar un número negativo para un byte sin signo.
Corto	Número decimal entre -32768 y 32767 (inclusive).
Corto sin signo	Número decimal entre 0 y 65535 (inclusive). No puede especificar un número negativo para un formato corto sin signo.
Lista de cortos sin signo	Uno o más números decimales entre 0 y 65535 (inclusive), separados por blancos. No puede especificar un número negativo para un formato corto sin signo.
Largo	Valor decimal entre -2147483648 y 2147483647 (inclusive).
Largo sin signo	Número decimal entre 0 y 4294967295 (inclusive). No puede especificar un número negativo para un formato largo sin signo.
Serie	Una serie de caracteres.
N/A	Indica que no es necesaria ninguna especificación, porque el cliente genera esta información.

Cada opción de DHCP se identifica mediante un código numérico.

Las RFC reservan las opciones de arquitectura 0 a 127 y la opción 255 para definiciones. El servidor DHCP, el cliente DHCP o ambos, utilizan las opciones de este conjunto. El administrador puede modificar algunas opciones de arquitectura. Otras opciones son para el uso exclusivo del cliente y del servidor.

Nota: Los valores hexadecimales no están permitidos para las opciones de arquitectura con formatos conocidos.

Las opciones que el administrador no puede o no debe configurar en el servidor DHCP incluyen las siguientes:

- 52** Carga excesiva de opción
- 53** Tipo de mensaje de DHCP
- 54** Identificador de servidor

55	Lista de peticiones de parámetros
56	Mensaje
57	Tamaño máximo de mensaje DHCP
60	Identificador de clase

Las opciones 128 a 254 representan opciones definidas por el usuario que los administradores pueden definir, para pasar información al cliente DHCP con el fin de implementar los parámetros de configuración específicos del sitio.

Además, IBM proporciona un conjunto de opciones, específicas de IBM, como la opción 192: TXT RR

El formato de una opción definida por el usuario es:

Sintaxis:

opción *código valor*

donde

código Cualquier código de opción de 1 a 254, salvo los códigos ya definidos en una RFC.

valor Debe ser siempre una serie. En el servidor, puede ser una serie ASCII o hexadecimal. Sin embargo, en el cliente aparece siempre como una serie hexadecimal tal como se pasa al programa de proceso.

El servidor pasa el valor especificado al cliente. No obstante, es preciso crear un programa o un archivo de mandatos para procesar el valor.

Opciones básicas proporcionadas al cliente

Se proporcionan al cliente las siguientes opciones básicas. Consulte “Formatos de opción” en la página 515 para ver una descripción del formato de configuración.

1 Máscara de subred Esta opción se especifica sólo en el servidor DHCP. La máscara de subred del cliente, especificada en una notación decimal con puntos de 32 bits. Aunque no es obligatorio, en la mayoría de configuraciones el servidor DHCP debe enviar la opción 1, máscara de subred, a los clientes DHCP. La operación del cliente puede ser imprevisible si el cliente no recibe una máscara de subred del servidor DHCP y supone una máscara de subred que no es la adecuada para la subred. Si no se especifica, el cliente utiliza las máscaras de subred por omisión:

- Red de clase A 255.0.0.0
- Red de clase B 255.255.0.0
- Red de clase C 255.255.255.0

Formato de opción: direcciones IP

2 Desplazamiento de tiempo Esta opción se especifica sólo en el servidor DHCP. El desplazamiento (en segundos) de la subred del cliente respecto de la Hora universal coordinada (CUT). El desplazamiento es un entero con signo de 32 bits.

Formato de opción: largo

- 3** **Direccionador** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (por orden de preferencia) de los direccionadores en la subred del cliente.
- Formato de opción: direcciones IP
- 4** **Servidor horario** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (por orden de preferencia) de los servidores horarios disponibles para el cliente.
- Formato de opción: direcciones IP
- 5** **Servidor de nombres** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (por orden de preferencia) de los servidores de nombres IEN 116 disponibles para el cliente.
- Nota:** Ésta no es la opción de Servidor de nombres de dominio. Utilice la Opción 6 para especificar un Servidor de nombres de dominio.
- Formato de opción: direcciones IP
- 6** **Servidor de nombres de dominio** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (por orden de preferencia) de los servidores de Sistema de nombres de dominio disponibles para el cliente.
- Formato de opción: direcciones IP
- Nota:** Si se ha configurado Dynamic-Address en una interfaz PPP, tal vez pueda recuperar una dirección DNS primaria y secundaria, utilizando IPCP desde un Proveedor de servicios Internet (ISP). Para pasar estas direcciones DNS a los clientes DHCP de la opción 6, debe configurar la dirección de interfaz IP no numerada (como 0.0.0.n) que corresponde a la interfaz de Dirección dinámica. El servidor DHCP convertirá este valor a las direcciones recuperadas cuando el cliente envíe una petición. Si el cliente DHCP ha solicitado su información de configuración del servidor antes de que se activase la interfaz PPP, el cliente tendrá que reiniciar o renovar su alquiler para recibir las direcciones DNS aprendidas.
- 7** **Servidor de anotaciones cronológicas** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (por orden de preferencia) de los servidores de anotaciones cronológicas UDP MIT-LCS disponibles para el cliente.
- Formato de opción: direcciones IP
- 8** **Servidor de cookies** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (por orden de preferencia) de la cookie, o los servidores de cuota del día disponibles para el cliente.
- Formato de opción: direcciones IP
- 9** **Servidor LPR** Esta opción se puede especificar en el cliente DHCP y en el servidor DHCP. No obstante, si se especifica sólo en el cliente DHCP, la configuración estará incompleta. Las direcciones IP (por orden de preferencia) de los servidores de impresoras de líneas disponibles para el cliente. La Opción 9 elimina la necesidad de que los clientes especifiquen la variable de entorno LPR_SERVER.

- Formato de opción: direcciones IP
- 10 Servidor de estampación** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (por orden de preferencia) de los servidores de estampación de imagen disponibles para el cliente.
- Formato de opción: direcciones IP
- 11 Servidor de ubicación de recursos** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (por orden de preferencia) de los servidores RLP (Ubicación de recursos) disponibles para el cliente. Los servidores RLP permiten que los clientes localicen recursos que proporcionen un servicio determinado, como un servidor de nombres de dominio.
- Formato de opción: direcciones IP
- 12 Nombre de sistema principal** Esta opción se puede especificar en el cliente DHCP y en el servidor DHCP. Si el cliente DHCP no proporciona un nombre de sistema principal, el servidor DHCP pasará por alto la opción 12. Nombre de sistema principal del cliente (que puede incluir el nombre de dominio local). La longitud mínima para la opción de nombre de sistema principal es de 1 octeto, mientras que la máxima es de 32 caracteres. Vea las restricciones sobre el juego de caracteres en el documento RFC 1035.
- Formato de opción: serie
- 13 Tamaño de archivo de arranque** Esta opción se especifica sólo en el servidor DHCP. La longitud (en bloques de 512 octetos) del archivo de configuración de arranque por omisión para el cliente.
- Formato de opción: corto sin signo
- 14 Archivo de vuelco de mérito** Esta opción se especifica sólo en el servidor DHCP. El nombre de vía de acceso del archivo de vuelco de mérito, en el que la imagen de memoria del cliente se almacena si el cliente se cuelga. La vía de acceso adopta el formato de una serie de caracteres, que consiste en caracteres del juego de caracteres ASCII NVT (Terminal virtual de red). La longitud mínima es de 1 octeto.
- Formato de opción: serie
- 15 Nombre de dominio** Esta opción se puede especificar en el cliente DHCP y en el servidor DHCP. Si no se especifica ningún valor en el servidor DHCP en la opción 15, se necesita el cliente para proporcionar un valor para la opción 12, nombre de sistema principal, y para la opción 15, nombre de dominio. Esta instrucción puede aparecer en el ámbito global o en un ámbito de Subred, Clase o Cliente.
- Formato de opción: serie
- 16 Servidor de intercambio** Esta opción se especifica sólo en el servidor DHCP. La dirección IP del servidor de intercambio del cliente.
- Formato de opción: dirección IP
- 17 Vía de acceso de raíz** Esta opción se especifica sólo en el servidor DHCP. La vía de acceso que contiene el disco raíz del cliente. La vía de acceso adopta el formato de una serie de caracteres, que consiste en caracteres del juego de caracteres ASCII NVT. La longitud mínima es de 1 octeto.

Formato de opción: serie

- 18** **Vía de acceso de extensión** Esta opción se especifica sólo en el servidor DHCP. La opción de vía de acceso de extensión especifica una serie que se puede utilizar para identificar un archivo recuperable mediante el protocolo TFTP (Trivial File Transfer Protocol). La longitud mínima es de 1 octeto.

Formato de opción: serie

Opciones de parámetros de capa IP por sistema principal

- 19** **Reenvío IP** Esta opción se especifica sólo en el servidor DHCP. Habilite (1) o inhabilite (0) el reenvío por el cliente de sus paquetes de capa IP.

Formato de opción: Booleano

- 20** **Direccionamiento no local de origen** Esta opción se especifica sólo en el servidor DHCP. Habilite (1) o inhabilite (0) el reenvío por el cliente de sus datagramas de capa IP con rutas de origen no locales.

Formato de opción: Booleano

- 21** **Filtro de política** Esta opción se especifica sólo en el servidor DHCP. Par dirección IP-máscara de red que se utiliza para filtrar datagramas con rutas de origen no locales. El cliente descartará cualquier datagrama cuya dirección de salto siguiente no coincida con uno de los pares de filtro. La longitud mínima para la opción de filtro de política es de 8 octetos.

Formato de opción: pares de direcciones IP

- 22** **Tamaño máximo de reunión de datagramas** Esta opción se especifica sólo en el servidor DHCP. El tamaño máximo de datagrama que reunirá el cliente. El valor mínimo es 576.

Formato de opción: corto sin signo

- 23** **Tiempo de vida IP por omisión** Esta opción se especifica sólo en el servidor DHCP. Tiempo de vida (TTL) por omisión que el cliente utiliza en los datagramas de salida. TTL es un octeto con un valor de 1 a 255.

Formato de opción: byte sin signo

- 24** **Tiempo de espera de antigüedad de MTU de vía de acceso** Esta opción se especifica sólo en el servidor DHCP. Tiempo de espera, medido en segundos, que se utiliza para la antigüedad de los valores de Unidad máxima de transmisión (MTU) de vía de acceso descubiertos por el mecanismo descrito en el documento RFC 1191.

Formato de opción: largo sin signo

- 25** **Tabla de meseta de MTU de vía de acceso** Esta opción se especifica sólo en el servidor DHCP. Tabla de tamaños de MTU para solicitar en descubrimiento de MTU de vía de acceso, tal como está definida en el documento RFC 1191. El valor mínimo de MTU es 68. La longitud mínima de la opción de tabla de meseta de MTU de vía de acceso es de 2 octetos. El valor de la longitud debe ser múltiplo de 2.

Formato de opción: corto sin signo

Opciones de parámetros de capa IP por interfaz

- 26** **MTU de interfaz** Esta opción se especifica sólo en el servidor DHCP. Unidad máxima de transmisión (MTU) para solicitar en esta interfaz. El valor mínimo de MTU es 68.
Formato de opción: corto sin signo
- 27** **Todas las subredes son locales** Esta opción se especifica sólo en el servidor DHCP. El cliente supone (1) o no supone (0) que todas las subredes utilizan la misma MTU (Unidad máxima de transmisión). El valor 0 significa que el cliente supone que algunas subredes tienen unas MTU más pequeñas.
Formato de opción: Booleano
- 28** **Dirección de difusión** Esta opción se especifica sólo en el servidor DHCP. Dirección de difusión utilizada en la subred del cliente.
Formato de opción: dirección IP
- 29** **Realizar descubrimiento de máscara** Esta opción se especifica sólo en el servidor DHCP. El cliente realiza (1) o no realiza (0) el descubrimiento de máscara de subred mediante el protocolo ICMP (Internet Control Message Protocol).
Formato de opción: Booleano
- 30** **Suministrador de máscara** Esta opción se especifica sólo en el servidor DHCP. El cliente responde (1) o no responde (0) a las peticiones de máscara de subred mediante el protocolo ICMP (Internet Control Message Protocol).
Formato de opción: Booleano
- 31** **Realizar descubrimiento de direccionador** Esta opción se especifica sólo en el servidor DHCP. El cliente solicita (1) o no solicita (0) direccionadores que utilicen el descubrimiento de direccionador, tal como está definido en el documento RFC 1256.
Formato de opción: Booleano
- 32** **Dirección de solicitud de direccionador** Esta opción se especifica sólo en el servidor DHCP. Dirección a la que un cliente transmite peticiones de solicitud de direccionador.
Formato de opción: dirección IP
- 33** **Ruta estática** Esta opción se especifica sólo en el servidor DHCP. Las rutas estáticas (pares dirección de designación-direccionador, por orden de preferencia) que el cliente instala en su antememoria de direccionamiento. La primera dirección es la dirección de destino, y la segunda es el direccionador del destino. No especifique 0.0.0.0 como destino de ruta por omisión.
Formato de opción: pares de direcciones IP

Opciones de parámetros de capa de enlace por interfaz

- 34 Encapsulación de terminación** Esta opción se especifica sólo en el servidor DHCP. El cliente negocia (1) o no negocia (0) el uso de terminaciones al utilizar el protocolo ARP (Address Resolution Protocol). Para obtener más información, vea el documento RFC 893.
- Formato de opción: Booleano
- 35 Tiempo de espera de antememoria ARP** Esta opción se especifica sólo en el servidor DHCP. Tiempo de espera, en segundos, para las entradas de antememoria del protocolo APR (Address Resolution Protocol).
- Formato de opción: largo sin signo
- 36 Encapsulación Ethernet** Esta opción se especifica sólo en el servidor DHCP. Para una interfaz Ethernet, el cliente utiliza la encapsulación Ethernet IEEE 802.3 (1), descrita en el documento RFC 1042, o la encapsulación Ethernet V2 (0), descrita en el documento RFC 894.
- Formato de opción: Booleano

Opciones de parámetros de TCP

- 37 TTL por omisión de TCP** Esta opción se especifica sólo en el servidor DHCP. Tiempo de vida (TTL) por omisión que el cliente utiliza para enviar segmentos TCP.
- Formato de opción: byte sin signo
- 38 Intervalo de latencia TCP** Esta opción se especifica sólo en el servidor DHCP. Intervalo, medido en segundos, que el cliente espera antes de enviar un mensaje de latencia en una conexión TCP. El valor 0 indica que el cliente no envía mensajes de latencia, a menos que la aplicación los solicite.
- Formato de opción: largo sin signo
- 39 Basura de latencia TCP** Esta opción se especifica sólo en el servidor DHCP. El cliente envía (1) o no envía (0) mensajes de latencia TCP que contienen un octeto de basura para obtener compatibilidad con implementaciones anteriores.
- Formato de opción: Booleano

Opciones de parámetros de aplicaciones y servicios

- 40 Dominio de servicio de información de red** Esta opción se especifica sólo en el servidor DHCP. El dominio NIS (Servicio de información de red) del cliente. El dominio se formatea como una serie de caracteres, consistente en caracteres del juego de caracteres ASCII NVT. La longitud mínima es de 1 octeto.
- Formato de opción: serie
- 41 Dominio de servicio de información de red** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (por orden de preferencia) de los servidores NIS (Servicio de información de red) disponibles para el cliente.

Formato de opción: direcciones IP

- 42 Servidores NTP** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (por orden de preferencia) de los servidores NTP (Network Time Protocol) disponibles para el cliente.

Formato de opción: direcciones IP

- 43 Información específica de servidor** La opción 43 se especifica sólo en el servidor DHCP, que devuelve esta opción a un cliente que envía la opción 60, Identificador de clase. Clientes y servidores utilizan esta opción de información para intercambiar información específica del proveedor, que se especifica en la definición de opción de proveedor. Las consideraciones para utilizar la Opción 43 para encapsular la información sobre proveedores son:

- Para permitir la interoperatividad entre clientes y servidores de proveedores diferentes, cada proveedor debe documentar claramente el contenido de su opción 43, utilizando el formato estándar del documento RFC 2132.
- Cada proveedor debe indicar las opciones específicas que se pueden encapsular en la opción 43, en un formato que los servidores DHCP de otro proveedor puedan implementar con facilidad. Por ejemplo, el proveedor debería:
 - Representar esas opciones en tipos de datos ya definidos para las opciones DHCP o en otros tipos de datos definidos.
 - Elegir las opciones que se pueden codificar con facilidad en archivos de configuración para realizar intercambios con los servidores proporcionados por otros proveedores.
 - Ser fácil de soportar por todos los servidores.

Los servidores que no puedan interpretar la información específica del proveedor que ha enviado un cliente, deben hacer caso omiso de la misma. Los clientes que no reciban la información específica del proveedor deseada, deben intentar operar sin ella. Consulte los documentos RFC 2131 y RFC 2132 para obtener información adicional acerca de esta opción.

Nota: Debido a estas consideraciones, IBM utiliza las opciones 192 y 200 para sus propias opciones específicas.

Formato de opción: serie

- 44 Servidor de nombres NetBIOS a través de TCP/IP** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (por orden de preferencia) de los servidores de nombres NetBIOS (NBNS) disponibles para el cliente.

Formato de opción: direcciones IP

- 45 Servidor de distribución de datagramas NetBIOS a través de TCP/IP** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (por orden de preferencia) de los servidores de nombres de distribución de datagramas NetBIOS (NBDD) disponibles para el cliente.

Formato de opción: direcciones IP

- 46 Tipo de nodo NetBIOS a través de TCP/IP** Esta opción se especifica sólo en el servidor DHCP. Tipo de nodo utilizado para los clientes configurables NetBIOS a través de TCP/IP, tal como está descrito en los documentos RFC 1001 y RFC 1002. Los valores para especificar tipos de cliente incluyen:
- 0x1 Nodo B
 - 0x2 Nodo P
 - 0x4 Nodo M
 - 0x8 Nodo H
- Formato de opción: byte sin signo
- 47 Ámbito de NetBIOS a través de TCP/IP** Esta opción se especifica sólo en el servidor DHCP. Parámetro de ámbito de NetBIOS a través de TCP/IP para el cliente, tal como se especifica en los documentos RFC 1001/1002. La longitud mínima es de 1 octeto.
- Formato de opción: byte sin signo
- 48 Servidor de fonts de sistema X Window** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (por orden de preferencia) de los servidores de fonts de sistema X Window disponibles para el cliente.
- Formato de opción: direcciones IP
- 49 Window System Display Manager** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (por orden de preferencia) de los sistemas que ejecutan X Window System Display Manager que están disponibles para el cliente.
- Formato de opción: direcciones IP

Opciones de extensiones DHCP

- 50 Dirección IP solicitada** Esta opción se especifica sólo en el servidor DHCP. El servidor DHCP puede rechazar una petición de cliente DHCP de una dirección IP específica. Permite que el cliente solicite (DHCPDISCOVER) una dirección IP determinada.
- Formato de opción: N/A
- 51 Período de alquiler de dirección IP** Esta opción se puede especificar en el cliente DHCP y en el servidor DHCP. El cliente DHCP puede utilizar la opción 51 para alterar temporalmente el valor de defaultLeaseInterval que ofrece el servidor DHCP. Permite que el cliente solicite (DHCPDISCOVER o DHCPREQUEST) un período de alquiler para una dirección IP. En una respuesta (DHCPOFFER), un servidor DHCP utiliza la opción de ofrecer un período de alquiler. Esta opción puede especificarse en el ámbito global, de subred, de clase o de cliente. Utilice X'ffffff' para indicar un alquiler infinito (permanente).
- Formato de opción: largo sin signo
- 58 Valor de tiempo de renovación (T1)** Esta opción se especifica sólo en el servidor DHCP. Intervalo, en segundos, entre el tiempo en que el servidor asigna una dirección y el tiempo que el cliente realiza una transición al estado de renovación.

Formato de opción: largo sin signo

- 59 Valor de tiempo de revinculación (T2)** Esta opción se especifica sólo en el servidor DHCP. Intervalo, en segundos, entre el tiempo en que el servidor asigna una dirección y el tiempo que el cliente entra en el estado de revinculación.

Formato de opción: largo sin signo

- 60 Identificador de clase** Esta opción se especifica sólo en el servidor DHCP. El cliente genera esta información y no es preciso especificarla. Tipo y configuración del cliente, suministrada por el cliente al servidor. Por ejemplo, el identificador puede codificar la configuración de hardware del cliente que sea específica del proveedor. La información es una serie de n octetos, interpretados por servidores. Por ejemplo: hex: X'01' X'02' X'03'. Los servidores que no estén equipados para interpretar la información específica de la clase enviada por un cliente deben pasarla por alto. La longitud mínima es de 1 octeto.

Formato de opción: N/A

- 61 Identificador de cliente** Esta opción se puede especificar en el cliente DHCP y en el servidor DHCP. El cliente DHCP puede utilizar la opción 61 para especificar el identificador de cliente exclusivo. El servidor DHCP puede utilizar la opción 61 para indexar la base de datos de los vínculos de direcciones. Se espera que este valor sea exclusivo para todos los clientes en un dominio administrativo.

Formato de opción: serie

- 62 Nombre de dominio de NetWare/IP** Esta opción se especifica sólo en el servidor DHCP. Nombre de dominio Netware/IP Domain Name. La longitud mínima es de 1 octeto y la longitud máxima es de 255

Formato de opción: serie

- 63 NetWare/IP** Esta opción se especifica sólo en el servidor DHCP. Se utiliza un código de opción de propósito general para transmitir toda la información relacionada de NetWare/IP, salvo para el nombre de dominio de NetWare/IP. Se transmitirán varias subopciones de NetWare/IP utilizando el código de opción. La longitud mínima es de 1 octeto y la longitud máxima es de 255.

Formato de opción: serie

- 64 Nombre de dominio de NIS** Esta opción se especifica sólo en el servidor DHCP. Nombre de dominio de cliente de Network Information Service (NIS)+ V3. El dominio se formatea como una serie de caracteres, consistente en caracteres del juego de caracteres ASCII NVT. La longitud mínima es 1.

Formato de opción: serie

- 65 Servidores NIS** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (por orden de preferencia) de Network Information Service (servidores NIS+ V3 disponibles para el cliente).

Formato de opción: direcciones IP

- 66** **Nombre de servidor** Esta opción se especifica sólo en el servidor DHCP. Nombre de servidor TFTP (Trivial File Transfer Protocol) utilizado cuando el campo "sname" en la cabecera DHCP se ha utilizado para las opciones de DHCP.
Formato de opción: serie
- 67** **Nombre de archivo de arranque** Esta opción se especifica sólo en el servidor DHCP. Nombre del archivo de arranque cuando el campo de archivo en la cabecera DHCP se ha utilizado para las opciones de DHCP. La longitud mínima es 1.
Nota: Utilice esta opción para pasar un nombre de archivo de arranque a un cliente DHCP. Se requiere que el nombre de archivo de arranque contenga el nombre de vía de acceso calificado al completo y que tenga una longitud inferior a 128 caracteres. Por ejemplo: option 67 c:\path\boot_file_name. Este archivo contiene información que puede interpretarse de la misma manera que el campo de extensión de proveedor de 64 octetos en la respuesta BOOTP, con la excepción de que la longitud de archivo está limitada a 128 caracteres por la cabecera BootP.
Formato de opción: serie
- 68** **Dirección inicial** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (por orden de preferencia) de los agentes iniciales IP móviles disponibles para el cliente. La opción habilita un sistema principal móvil del que derivará una dirección inicial móvil y determina la máscara de subred para la red inicial. La longitud usual es de cuatro octetos, que contienen una dirección inicial de un agente inicial, pero la longitud puede ser cero. La longitud cero indica que no hay agentes iniciales disponibles.
Formato de opción: direcciones IP
- 69** **Servidores SMTP** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (por orden de preferencia) de los servidores SMTP (Simple Mail Transfer Protocol) disponibles para el cliente.
Formato de opción: direcciones IP
- 70** **Servidor POP3** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (por orden de preferencia) de los servidores POP (Post Office Protocol) disponibles para el cliente.
Formato de opción: direcciones IP
- 71** **Servidor NNTP** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (por orden de preferencia) de los servidores NNTP (Network News Transfer Protocol) disponibles para el cliente.
Formato de opción: direcciones IP
- 72** **Servidor WWW** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (por orden de preferencia) de los servidores WWW (World Wide Web) disponibles para el cliente.
Formato de opción: direcciones IP

- 73 Servidor Finger** Esta opción se especifica sólo en el servidor DHCP. Direcciones IP (por orden de preferencia) de los servidores Finger disponibles para el cliente.
Formato de opción: direcciones IP
- 74 Servidor IRC** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (por orden de preferencia) de los servidores IRC (Internet Relay Chat) disponibles para el cliente.
Formato de opción: direcciones IP
- 75 Servidor StreetTalk** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (por orden de preferencia) de los servidores StreetTalk disponibles para el cliente.
Formato de opción: direcciones IP
- 76 Servidor STDA** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (por orden de preferencia) de los servidores StreetTalk STDA (StreetTalk Directory Assistance) disponibles para el cliente.
Formato de opción: direcciones IP
- 77 Clase de usuario** Esta opción se especifica sólo en el servidor DHCP. Los clientes DHCP utilizan la opción 77 para indicar a los servidores de DHCP de qué clase es miembro el sistema principal. Es preciso entrar manualmente la clase de usuario en el archivo \DHCPD.CFG, como el valor de la opción 77, para recibir los parámetros definidos para la clase en un servidor DHCP. El archivo DHCPD.CFG está ubicado en el directorio ONDEMAND\SERVER\ETC.
Formato de opción: serie
- 78 Agente de directorios** Esta opción se especifica sólo en el servidor DHCP. DHCP (Dynamic Host Configuration Protocol) proporciona un marco para pasar información de configuración a los sistemas principales de una red TCP/IP. Las entidades que utilizan el protocolo SLP (Service Location Protocol) tienen que averiguar la dirección de los Agentes de directorios para realizar la transacción de mensajes. En otras instancias determinadas, puede que tengan que descubrir el ámbito y la autoridad de denominación correctos que deben utilizarse junto con los atributos de servicio y los URL que se intercambian utilizando el protocolo SLP. Un agente de directorios tiene un ámbito determinado y puede conocer acerca de los esquemas definidos por una autoridad de nombres específica.
Formato de opción: dirección IP
- 79 Ámbito de servicio** Esta opción se especifica sólo en el servidor DHCP. Esta extensión indica un ámbito que un agente de servicio debe utilizar, al responder a mensajes de Petición de servicio, según lo ha especificado el protocolo SLP.
Formato de opción: serie
- 80 Autoridad de denominación** Esta opción se especifica sólo en el servidor DHCP. Esta extensión indica una autoridad de denominación, que especifica la sintaxis de los esquemas que pueden utilizarse en los URL para su uso por entidades con el protocolo SLP.

Formato de opción: serie

Opciones específicas de IBM

IBM proporciona un conjunto de opciones, específicas de IBM, definidas dentro del rango definido por el usuario (128-254). Estas opciones se utilizan en lugar de definir una opción de proveedor (opción 43) para IBM. Es recomendable que no vuelva a definir estas opciones.

- 192** **TXT RR** Si se especifica esta opción en el servidor DHCP, se requiere que el usuario del cliente DHCP complete los campos de información del administrador del sistema. Nota: esta opción sólo está soportada por TCP/IP Versión 4.1 para clientes OS/2. Esta opción proporciona un máximo de cuatro etiquetas de texto o campos de entrada necesarios que el administrador del sistema puede especificar, como el nombre de un usuario, el número telefónico del usuario u otros campos que el programa de configuración de DDNS Client solicita al usuario. Estos campos permiten que el administrador del sistema identifique la persona que ha configurado el nombre de sistema principal u otros datos. El programa de configuración de DDNS no visualiza estos campos, a menos que el administrador del sistema los especifique. Esta información se almacena en un registro de texto en el DNS. Los pares de etiquetas de campo y datos son necesarios para encajar en un único registro de recurso TXT. El espacio disponible está dividido de manera equitativa entre los pares. El valor también se actualiza en el archivo DDNSCLI.CFG en el cliente de Dirección dinámica.

Formato de opción: serie

Opciones de proveedor

El protocolo DHCP proporciona una manera de suministrar información específica del proveedor a un cliente DHCP, utilizando las opciones de arquitectura de RFC 43 y 60.

- 60** La **Opción 60** está configurada en un cliente DHCP y se envía al servidor DHCP para identificar el cliente como uno de un proveedor específico.
- 43** La **Opción 43** se configura en el servidor DHCP para definir la información específica del proveedor que se debe devolver al cliente, como respuesta a la petición de la opción 60 del cliente. Para el servidor DHCP de Código común, la opción 43 se configura con el mandato add vendor-option. Una opción de proveedor sólo se define en el ámbito global. La opción de proveedor consiste en el nombre del proveedor y los datos de opción. Los datos de opción tienen dos formatos:

Datos hexadecimales

Se entra con el nombre de proveedor, cuando se emite el mandato add vendor-option. Los datos hexadecimales deben entrarse como una serie hexadecimal con blancos entre los bytes: "01 AA 55"

Opciones

Puede añadirse cualquier opción de DHCP a un ámbito de opción de proveedor, por el mandato add option.

Nota: Los datos hexadecimales y las opciones son mutuamente excluyentes en una definición de proveedor. Puede definir uno u otro, pero no ambos.

Configuración de IP para DHCP

Para que el servidor DHCP asigne satisfactoriamente las direcciones IP y la información de configuración para los clientes en una subred añadida, IP tendrá que configurarse de la manera adecuada. Esto se producirá cuando el servidor DHCP esté conectado directamente a una subred que está configurada para dar soporte.

Si se utiliza un agente de BOOTP Relay para reenviar mensajes de petición de DHCP a este servidor DHCP, puede que no haya una configuración de IP necesaria para dar soporte a una subred que no está conectada directamente al servidor.

Adición de una dirección IP

Una dirección IP que caiga en la subred de DHCP configurada, tendrá que añadirse a la interfaz de conexión. Si hay varias direcciones definidas en esa interfaz, la dirección añadida para DHCP debe ser la **última** añadida. IP sólo presentará un mensaje DHCP DISCOVER de difusión al servidor, como si llegara a la primera dirección encontrada para esa interfaz.

Nota: La primera dirección encontrada en una interfaz es la **última** dirección añadida a la interfaz.

Ejemplo:

- DHCP ha añadido una subred de la manera siguiente:

```
DHCP Server config>list subnet all
subnet      subnet      subnet      starting      ending
name        address     mask        IP Addr       IP Addr
-----
net-one     192.168.8.0 255.255.255.0 192.168.8.2   192.168.8.50
```

- IP necesitará lo siguiente:

```
IP config>add address
Which net is this address for [0]? 0
New address []? 192.168.8.1
Address mask [255.255.255.0]?

IP config>list add
IP addresses for each interface:
intf  0  192.168.8.1  255.255.255.0  Local wire broadcast, fill 1
intf  1                                     IP disabled on this interface
intf  2  0.0.0.2     255.255.255.255  Local wire broadcast, fill 1
intf  3                                     IP disabled on this interface
```

Utilización de Simple-Internet-Access de IP

Si Simple-Internet-Access está habilitado en IP y DHCP no se ha configurado anteriormente, la siguiente configuración se generará automáticamente en el servidor DHCP. Simple-Internet-Access también configurará automáticamente la característica NAT y otros filtros IP y controles de acceso. Si DHCP ya está configurado, no habrá cambios/adiciones a la configuración de DHCP. Consulte Using Simple Internet Access en el capítulo “Using IP” del manual *Consulta de configuración y supervisión de protocolos Volumen 1* para obtener más información y conocer las restricciones existentes.

Utilización del servidor DHCP

- IP se ha configurado de la manera siguiente:

```
IP config>enable simple-internet-access
Interface to Service Provider [0]? 3
SIMPLE-INTERNET-ACCESS enabled on interface 3

IP config>add address
Which net is this address for [0]? 0
New address []? 192.168.8.1
Address mask [255.255.255.0]?

IP config>list add
IP addresses for each interface:
intf  0  192.168.8.1      255.255.255.0  Local wire broadcast, fill 1
intf   1                               IP disabled on this interface
intf   2                               IP disabled on this interface
intf   3  0.0.0.3        255.255.255.255  Local wire broadcast, fill 1
                                           SIMPLE-INTERNET-ACCESS Enabled
```

- El servidor DHCP tendrá generada la siguiente configuración:

```
DHCP Server config> list global
.
.
DHCP Server enabled: Yes
.
.
DHCP Server config>list subnet all
subnet  subnet      subnet      starting    ending
name    address          mask        IP Addr     IP Addr
-----
simple-net 192.168.8.0     255.255.255.0  192.168.8.2  192.168.8.50

DHCP Server config>list option subnet
Enter the subnet name []? simple-net
option  option
code   data
-----
1      255.255.255.0
3      192.168.8.1
6      0.0.0.3
```

Configuración de ejemplo de servidor DHCP

Archivo de texto ASCII

Esta sección proporciona una configuración de servidor DHCP típica en formato de texto ASCII. Este ejemplo es estrictamente ilustrativo y muestra una configuración en un formato que puede resultarle familiar. El IBM 2216 no da soporte a las configuraciones ASCII.

Puede utilizar los números visualizados como bloque (**1**) para relacionar las funciones descritas en este ejemplo en ASCII con la configuración de talk 6 equivalente que se muestra en la “Configuración de OPCON (Talk 6)” en la página 533.

1 Configuración de parámetros de servidor

```

leaseTimeDefault      120                # 120 minutes
leaseExpireInterval   20 seconds
supportBOOTP          yes
supportUnlistedClients yes

```

2 Opciones globales. Pasadas a todos los clientes salvo alteradas temporalmente en un ámbito inferior.

```

option 15      "raleigh.ibm.com"      # domain name
option 6       9.67.1.5                # dns server

class manager
{
  option 48    6.5.4.3
  option 9     9.37.35.146
  option 210   "manager_authority"    # site specific option given to all managers
}

```

3 Opciones de proveedor

```

vendor XI-clients hex"01 02 03"

vendor XA-clients
{
  option 23 100 # IP TTL
}

```

4 Subred típica

```

subnet 9.2.23.0 255.255.255.0      9.2.23.120-9.2.23.126
{
  option 28      9.2.23.127        # broadcast address
  option 9       5.6.7.8
  option 51     200
}

```

5 Gestor de clase definido en ámbito de subred. La opción 9 prevalecerá sobre la opción 9 especificada en la clase de gestor global.

```

class manager
{
  option 9     9.2.23.98
}

```

Utilización del servidor DHCP

6 Los programadores tienen su propio rango de subred.

```
class developers 9.2.23.125-9.2.23.126
{
    option 51 -1 # infinite lease.
    option 9 9.37.35.1 # printer used by the developers
}
}
```

7 Ejemplo de cliente que acepta cualquier dirección pero tiene su propio conjunto de opciones.

```
client 6 0x10005aa4b9ab ANY
{
    option 51 999
    option 1 255.255.255.0
}
```

8 Excluir una dirección del servicio.

```
client 0 0 9.2.23.121
```


Configuración de OPCON (Talk 6)

A continuación se muestra un ejemplo de la misma configuración utilizando talk 6.

1 Configuración de parámetros de servidor

```
Config>f dhcp-server
DHCP server user configuration
DHCP Server config> enable dhcp
DHCP Server config>

DHCP Server config> set lease-time-default hours 2
DHCP Server config>set lease-expire-interval seconds 20
DHCP Server config>set support-bootp yes
DHCP Server config>set support-unlisted-clients global yes
```

```
DHCP Server config>li glob
DHCP server Global Parameters
=====
```

DHCP server enabled: Yes

Balance: No subnet groups defined

Inorder: No subnet groups defined

Canonical: No

Lease Expire Interval: 20 second(s)
Lease Time Default: 2 hour(s)

Support BOOTP Clients: Yes
Bootstrap Server: Not configured

Support Unlisted Clients: Yes

Ping Time: 1 second(s)
Used IP Address Expire Interval: 15 minute(s)

2 Opciones globales. Pasadas a todos los clientes salvo alteradas temporalmente en un ámbito inferior.

```
DHCP Server config>add option global 15 raleigh.ibm.com
DHCP Server config>add option global 6 9.67.1.5
```

```
DHCP Server config>li option global
option option
code data
```

```
-----
15    raleigh.ibm.com
6     9.67.1.5
```

Utilización del servidor DHCP

```
DHCP Server config>add class global
Enter the class name []? manager
Class record with name manager has been added

DHCP Server config>add option class-global
Enter the class name []? manager
Enter the option code [1]? 48
Enter the option data []? 6.5.4.3

DHCP Server config>add option class-global 9 9.37.35.146
DHCP Server config>add option class-global manager 210 manager_authority

DHCP Server config>li class global manager
class
name
-----
manager

Number of Options: 3
option option
code data
-----
48      6.5.4.3
9       9.37.35.146
210    manager_authority

3 Opciones de proveedor

DHCP Server config>add vendor-option XI-client
Enter the vendor hex data []? 01 02 03
Vendor-option record with name XI-client has been added

DHCP Server config> add vendor-option XA-client
Enter the vendor hex data []?
Vendor-option record with name XA-client has been added
DHCP Server config> add option vendor-option XA-client 23 100

DHCP Server config>li vendor-option all
vendor hex
name data
-----
XI-client 01 02 03
XA-client
DHCP Server config>li vendor-option det XA-client
vendor hex
name data
-----
XA-client

Number of Options: 1
option option
code data
-----
23      100
```

4 Subred típica

```

DHCP Server config>add subnet
Enter the subnet name []? sub1
Enter the IP subnet []? 9.2.23.0
Enter the IP subnet mask [255.255.255.0]?
Enter start of IP address range [9.2.23.1]? 9.2.23.120
Enter end of IP address range [9.2.23.150]? 9.2.23.126
Enter the subnet group name []?
Subnet record with name sub1 has been added
DHCP Server config>
DHCP Server config> add option subnet
Enter the subnet name []? sub1
Enter the option code []? 28
Enter the option data []? 9.2.23.127
DHCP Server config> add option subnet 9 5.6.7.8
DHCP Server config>add option subnet sub1 51 200

```

```

DHCP Server config>add class subnet
Enter the subnet name []? sub1
Enter the class name []? manager
Enter start of IP address range []?
Class record with name manager has been added

```

```

DHCP Server config>add option class-subnet sub1 manager
Enter the option code [1]? 9
Enter the option data []? 9.2.23.98

```

6 Los programadores tienen su propio rango de subred.

```

DHCP Server config>add class subnet
Enter the subnet name []? sub1
Enter the class name []? developers
Enter start of IP address range []? 9.2.23.125
Enter end of IP address range []? 9.2.23.126
Class record with name developers has been added

```

```

DHCP Server config>add option class-subnet sub1 developers 51 -1
DHCP Server config>add option class-subnet sub1 developers 9 9.37.35.1

```

Utilización del servidor DHCP

```
DHCP Server config>li subnet detailed sub1
subnet      subnet      subnet      starting    ending
name        address     mask        IP Addr     IP Addr
-----
sub1        9.2.23.0   255.255.255.0  9.2.23.120  9.2.23.126
```

Number of Classes: 2

class
name

manager

Number of Options: 1

option option
code data

9 9.2.23.98

developers

starting IP address: 9.2.23.125

ending IP address: 9.2.23.126

Number of Options: 2

option option
code data

51 -1
9 9.37.35.1

Number of Options: 3

option option
code data

28 9.2.23.127
9 5.6.7.8
51 200

7 Ejemplo de cliente que acepta cualquier dirección pero tiene su propio conjunto de opciones

```
DHCP Server config>add client global
Enter the client name []? any-addr
Enter the client's hardware type (0 - 21) [1]? 6
Enter the client ID (MAC address or string) []? 10005aa4b9ab
Enter the client's IP address (IP address, any, none) []? any
```

```
DHCP Server config>add option client-global any-addr 51 999
DHCP Server config>add option client-global any-addr 1 255.255.255.0
```

8 Excluir una dirección del servicio.

```
Enter the client name []? excl-addr
Enter the client's hardware type (0 - 21) [1]? 0
Enter the client ID (MAC address or string) []? 0
Enter the client's IP address (IP address, any, none) []? 9.2.23.121
```

```
DHCP Server config>li cli all
client      client client      attached  IP
name        type  identifier  to subnet address
-----
any-addr    6     10005aa4b9ab          Any
excl-addr   0     0                9.2.23.121
```

```
DHCP Server config>li client global any-addr
client      client client      IP
name        type  identifier  address
-----
any-addr    6     10005aa4b9ab          Any
```

```
Number of Options: 2
option option
code  data
-----
51    999
1     255.255.255.0
```


Configuración y supervisión del servidor DHCP

Este capítulo describe cómo utilizar la los mandatos operativos y de configuración del servidor DHCP y contiene las secciones siguientes:

- “Acceso al entorno de configuración de servidor DHCP”
- “Mandatos de configuración del servidor DHCP”
- “Acceso al entorno de supervisión de servidor DHCP” en la página 572
- “Mandatos de supervisión del servidor DHCP” en la página 573

Acceso al entorno de configuración de servidor DHCP

Utilice el siguiente procedimiento para acceder al proceso de *configuración* del servidor DHCP.

1. En el indicador OPCON, entre **talk 6**. Por ejemplo:

```
* talk 6
Config>
```

Después de entrar el mandato **talk 6**, el indicador Config (Config>) se visualiza en la terminal. Si el indicador no aparece al entrar la configuración por primera vez, pulse de nuevo **Return**.

2. En el indicador Config, entre el mandato **feature dhcp-server** para acceder al indicador DHCP Server config>.

Mandatos de configuración del servidor DHCP

Tabla 62. Resumen de los mandatos de configuración del servidor DHCP

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxiv.
Add	Añade una clase, un cliente, una subred o una opción de proveedor.
Change	Cambia la definición de una clase, un cliente, una subred o una opción de proveedor.
Default	Devuelve determinadas variables globales a sus valores por omisión.
Delete	Suprime una clase, una subred o una opción de proveedor.
Disable	Inhabilita globalmente el servidor DHCP.
Enable	Habilita globalmente el servidor DHCP.
List	Lista las definiciones globales o de una clase, un cliente, una subred o una opción de proveedor.
Set	Establece las definiciones para los parámetros globales o las opciones en un ámbito específico.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiv.

Add

Utilice el mandato **add** para añadir una clase, una subred o una opción de proveedor.

Sintaxis:

```
add                class
                   client
                   option
                   subnet
                   vendor-option
```

class *ámbito* [*nombre_subred*] *nombre_clase* [*inicio_rango*] [*fin_rango*]

Define una clase.

ámbito Especifica el ámbito al que se añade la clase.

Valores válidos: global o subnet

Valor por omisión: ninguno

nombre_subred

Esto sólo es válido si el valor de **ámbito** es *subnet*. Indica el nombre de la subred a la que se añade la clase.

Valores válidos: cualquier nombre de subred existente

Valor por omisión: ninguno

nombre_clase

Indica el nombre de la clase.

Valores válidos: una serie ASCII de una longitud máxima de 40 caracteres

Valor por omisión: ninguno

inicio_rango

Esto sólo es válido si el valor de **ámbito** es *subnet*. Especifica la dirección IP inicial para la agrupación de direcciones IP a la que se asignarán los clientes.

Valores válidos: cualquier dirección IP válida en el rango de la subred a la que se añade la clase.

Valor por omisión: primera dirección IP del rango de subred perteneciente a la subred especificada.

fin_rango

Esto sólo es válido si el valor de **ámbito** es *subnet*. Especifica la dirección IP final para la agrupación de direcciones IP a la que se asignarán los clientes.

Valores válidos: cualquier dirección IP válida en el rango de la subred a la que se añade la clase. Este valor debe ser mayor que el valor especificado para **inicio_rango**.

Valor por omisión: la dirección IP inicial más 5 del rango de subred perteneciente a la subred especificada. Si la dirección IP resultante ya no está dentro del rango de subred, el valor por omisión es la dirección IP final del rango de subred.

Mandatos de configuración de servidor DHCP (Talk 6)

Ejemplo:

```
DHCP Server config> add class global
Enter class name? ClassA

DHCP Server config> add class subnet
Enter the subnet name[]? subA
Enter class name[]? ClaA
Enter start of IP address range[10.1.1.1]?
Enter end of IP address range[10.1.1.6]?
```

client *ámbito [nombre_subred] nombre_cliente tipo-id valor-id dirección*

Define un cliente

ámbito Especifica el ámbito al que se añade el cliente.

Valores válidos: global o subnet

Valor por omisión: ninguno

nombre-subred

Sólo es válido si el valor de **ámbito** es *subnet*. Indica el nombre de la subred a la que se añade el cliente.

Valores válidos: cualquier nombre de subred existente

Valor por omisión: ninguno

nombre-cliente

Indica el nombre del cliente.

Valores válidos: cualquier serie ASCII de 10 caracteres

Valor por omisión: ninguno

tipo-id

Indica el tipo de hardware del cliente. Los tipos de hardware definidos en el documento RFC 1340 que son aplicables al IBM 2216 se muestran abajo como valores válidos.

Valores válidos:

0 No especificado. Indica un nombre simbólico para el cliente.

1 Ethernet

6 Redes IEEE 802 (incluida la Red en Anillo 802.5)

Valor por omisión: 1

valor-id Especifica el identificador de cliente. Si **tipo-id** es *0*, **id-value** es una serie de 64 caracteres. De lo contrario, **id-value** es una dirección MAC.

Nota: Un **tipo-id** de *0* y un **valor-id** de *0* indica que el servidor no debe distribuir la dirección IP especificada.

Valores válidos: 0 ó cualquier dirección MAC válida (12 dígitos hexadecimales)

Valor por omisión: ninguno

dirección Especifica la dirección IP que se debe suministrar al cliente o una serie de caracteres que indica que no se dará servicio al cliente o que se puede suministrar al cliente con cualquier dirección de la agrupación de direcciones IP.

Mandatos de configuración de servidor DHCP (Talk 6)

Valores válidos:

cualquier dirección IP válida En formato decimal con puntos. Si el cliente está definido en un ámbito de subred, la dirección IP debe estar dentro del rango de subred.

none Indica que no se dará servicio al cliente coincidente

any Indica que se puede suministrar al cliente cualquier dirección IP de la agrupación de subred.

Valor por omisión: ninguno

Nota: Un **tipo-id** de 0 y un **valor-id** de 0 indican que el servidor no debe distribuir la dirección IP especificada.

Ejemplo:

```
DHCP Server config> add client global
Enter the client name []? ClientA
Enter the client's hardware type (0 - 21) [1]? 0
Enter the client ID (MAC address or string) []? ClientA
Enter the client's IP address (IP address, any, none) []? 9.1.1.1
Client record with name ClientA has been added
```

```
DHCP Server config> add client subnet
Enter the subnet name []? subA
Enter the client name []? CliA
Enter the client's hardware type (0 - 21) [1]? 1
Enter the client ID (MAC address or string) []? 400000000010
Enter the client's IP address (IP address, any, none) []? 10.1.1.10
Client record with name CliA has been added
```

option *ámbito* [*nombre-subred*] [*nombre-clase*] [*nombre-cliente*] [*nombre-proveedor*]
código datos

Define una opción. Las opciones pueden existir globalmente, o dentro del ámbito de una subred, clase, cliente u opción de proveedor.

ámbito Especifica el ámbito al que se añade la opción.

Valores válidos:

- class-global
- class-subnet
- client-global
- client subnet
- global
- subnet
- vendor-option

Valor por omisión: ninguno

nombre-subred

Sólo es válido si el valor de **ámbito** es *subnet*, *class-subnet* o *client-subnet*. Indica el nombre de la subred a la que se añade el cliente.

Valores válidos: cualquier nombre de subred existente

Valor por omisión: ninguno

nombre-clase

Sólo es válido si el valor de **ámbito** es *class-global* o *class-subnet*. Indica el nombre de la clase a la que se añade la opción.

Valores válidos: cualquier nombre de clase existente

Valor por omisión: ninguno

nombre-cliente

Sólo es válido si el valor de **ámbito** es *client-global* o *client-subnet*. Indica el nombre del cliente al que se añade la opción.

Valores válidos: cualquier nombre de cliente existente

Valor por omisión: ninguno

nombre-proveedor

Sólo es válido si el valor de **ámbito** es *vendor-option*. Indica el nombre del proveedor al que se añade la opción.

Valores válidos: cualquier nombre de proveedor existente

Valor por omisión: ninguno

código

Especifica el código de opción. Las opciones de DHCP están definidas en el documento RFC 2132. Consulte "Opciones de DHCP" en la página 515 para ver una descripción de las opciones y sus formatos.

Valores válidos: 1 - 255

Valor por omisión: 1

datos

Especifica los datos de opción. Los datos de opción pueden definirse de tres maneras.

- Series ASCII para formatos específicos definidos en el documento RFC 2132.
- Conversión hexadecimal durante la inicialización. Los datos se deben entrar como *hex: 01 aa 04*.
- Serie de caracteres. Los datos se deben entrar como *abcdef*.

Mandatos de configuración de servidor DHCP (Talk 6)

Ejemplo:

```
DHCP Server config> add option global
Enter the option code [1]? 3
Enter the option data []? 9.167.100.1
```

Ejemplo:

```
DHCP Server config> add option subnet
Enter the subnet name []? subA
Enter the option code [1]? 3
Enter the option data []? 9.167.100.1
```

Ejemplo:

```
DHCP Server config> add option class-global
Enter the class name []? ClassA
Enter the option code [1]? 3
Enter the option data []? 9.167.100.1
```

Ejemplo:

```
DHCP Server config> add option client
Enter the client name []? ClientA
Enter the option code [1]? 3
Enter the option data []? 9.167.100.1
```

Ejemplo:

```
DHCP Server config> add option class-subnet
Enter the subnet name []? subA
Enter the class name []? ClaA
Enter the option code [1]? 3
Enter the option data []? 9.167.100.1
```

Ejemplo:

```
DHCP Server config> add option client-subnet
Enter the subnet name []? subA
Enter the client name []? CliA
Enter the option code [1]? 3
Enter the option data []? 9.167.100.1
```

Ejemplo:

```
DHCP Server config> add option vendor-option
Enter the vendor name []? 200
Enter the option code [1]? 85
Enter the option data []? hex:01 AA 04
```

Ejemplo:

```
DHCP Server config> add option vendor-option
Enter the vendor name []? 200
Enter the option code [1]? 86
Enter the option data []? 9.67.85.4
```

subnet *nombre-subred dirección-subred máscara-subred inicio-rango fin-rango*
[nombre_grupo_subredes] [prioridad_grupo_subredes] [list-política]
Define una subred.

nombre-subred

Indicates el nombre de la subred.

Valores válidos: cualquier serie ASCII de 10 caracteres

Valor por omisión: ninguno

dirección-subred

Especifica la dirección de la subred. La dirección se especifica en formato decimal con puntos.

Valores válidos: cualquier dirección de subred IP válida

Valor por omisión: ninguno

máscara-subred

Especifica la máscara de dirección de subred. La dirección de subred debe estar en la máscara de subred y no puede contener un número de bits mayor que el de la máscara.

Valores válidos: cualquier máscara IP válida en formato decimal con puntos

Valor por omisión: se calcula según la dirección de subred

inicio-rango

Especifica la dirección IP inicial de la agrupación de direcciones IP que este servidor administrará para esta subred. Si no se especifica *inicio-rango*, el servidor administrará todas las direcciones de la subred.

Valores válidos: cualquier dirección de sistema principal IP válida en la subred especificada, en formato decimal con puntos

Valor por omisión: la primera dirección IP de la subred

fin-rango Especifica la dirección IP final de la agrupación de direcciones IP que este servidor administrará para esta subred.

Valores válidos: cualquier dirección de sistema principal IP válida en la subred especificada, en formato decimal con puntos

Valor por omisión: **inicio-rango** más 50. Si la dirección IP resultante ya no está dentro del rango de subred, el valor por omisión es la última dirección IP de la subred.

nombre-grupo-subredes

Especifica el nombre de grupo de subredes al que pertenece esta subred.

Valores válidos: cualquier serie ASCII de una longitud máxima de 64 caracteres

Valor por omisión: ninguno

prioridad-grupo-subredes

Especifica la prioridad de esta subred en el grupo de subredes. Esta prioridad se utiliza para determinar el orden en que se asignan las direcciones dentro de un grupo de subredes específico.

Valores válidos: 1 - 65535

Valor por omisión: 1

lista-política

Identifica a qué lista de direcciones de política, Balance o Inorder, al que se añadirá el grupo de subredes. Si el grupo

Mandatos de configuración de servidor DHCP (Talk 6)

de subredes existe ya en una lista y se especifica la otra, el grupo de subredes se moverá a la nueva lista.

Valores válidos: Inorder o Balance

Valor por omisión: si es una subred nueva, el valor por omisión es Inorder. De lo contrario, es la lista de políticas actual a la que pertenece el grupo de subredes.

Ejemplo:

```
DHCP Server config> add subnet
Enter the subnet name []? subA
Enter the IP subnet []? 10.1.1.0
Enter the IP subnet mask [255.255.255.0]?
Enter start of IP address range [10.1.1.1]?
Enter end of IP address range [10.1.1.31]?
Enter the subnet group name []? group1
Enter the subnet group priority (1 - 65535) [1]?
Enter the access policy list (Inorder or Balance) [Inorder]?
Subnet record with name sub1 has been added
Subnet group group1 is being added to the Inorder List
```

vendor-option *nombre_proveedor* [*valor_hex*]

Añade una opción de proveedor. Hay dos maneras de proporcionar datos de opción de proveedor:

- Entre los datos hexadecimales cuando se le solicite
- Añada opciones específicas al proveedor utilizando el mandato **add option vendor**. Consulte la información sobre las opciones en la página 542.

nombre_proveedor

Especifica el nombre del proveedor.

Valores válidos: una serie ASCII de una longitud máxima de 40 caracteres

Valor por omisión: ninguno

valor_hex Especifica la serie ASCII hexadecimal que representa el valor hexadecimal de la parte de datos de la opción.

Valores válidos: cualquier serie hexadecimal válida en el formato siguiente: *01 aa 04*

Valor por omisión: ninguno

Ejemplo:

```
DHCP Server config> add vendor-option
Enter the vendor name []? XA-client
Enter the vendor hex data [] 01 aa 04?
Vendor-option record with name XA-client has been added
```

Change

Utilice el mandato **change** para modificar la configuración de una clase, un cliente, una subred o una opción de proveedor.

Sintaxis:

change class

client
subnet
vendor-option

class *ámbito* [*nombre_subred*] *nombre_clase* *nuevo_nombre_clase*
[*nuevo_inicio_rango*] [*nuevo_fin_rango*]

Modifica una clase.

ámbito Especifica el ámbito de la clase que se modifica.

Valores válidos: global o subnet

Valor por omisión: ninguno

nombre-subred

Sólo es válido si el valor de **ámbito** es *subnet*. Indica el nombre de la subred a la que pertenece la clase.

Valores válidos: cualquier nombre de subred existente.

Valor por omisión: ninguno

nombre-clase

Indica el nombre de la clase.

Valores válidos: nombre de una clase existente

Valor por omisión: ninguno

nuevo-nombre-clase

Indica el nuevo nombre de la clase.

Valores válidos: una serie ASCII de una longitud máxima de 40 caracteres

Valor por omisión: nombre de clase existente

nuevo-inicio-rango

Sólo es válido si el valor de **ámbito** es *subnet*. Especifica la nueva dirección IP inicial para la agrupación de direcciones IP a la que se asignarán los clientes.

Valores válidos: cualquier dirección IP dentro del rango de subred

Valor por omisión: inicio de rango existente

nuevo-fin-rango

Especifica la nueva dirección IP final para la agrupación de direcciones IP a la que se asignarán los clientes.

Valores válidos: cualquier dirección IP válida dentro del rango de subred, mayor que **nuevo-fin-rango**

Valor por omisión: fin de rango existente

Mandatos de configuración de servidor DHCP (Talk 6)

Ejemplo:

```
DHCP Server config> change class global  
Enter the class name []? ClassA  
Enter the new class name [ClassA]?
```

Ejemplo:

```
DHCP Server config> change class subnet  
Enter the subnet name []? subA  
Enter the class name []? ClAa  
Enter the new class name [ClAa]?  
Enter start of IP address range [10.1.1.1]?  
Enter end of IP address range [10.1.1.6]?
```

client *ámbito [nombre_subred] nombre_cliente nuevo-nombre_cliente nuevo-tipo-id nuevo-valor-id nueva-dirección*

Modifica un cliente

ámbito Especifica el ámbito del cliente que se modifica.

Valores válidos: global o subnet

Valor por omisión: ninguno

nombre-subred

Sólo es válido si el valor de **ámbito** es *subnet*. Indica el nombre de la subred a la que pertenece el cliente.

Valores válidos: cualquier nombre de subred existente

Valor por omisión: ninguno

nombre-cliente

Indica el nombre del cliente.

Valores válidos: un nombre de cliente existente

Valor por omisión: ninguno

nuevo-nombre-cliente

Indica el nuevo nombre del cliente.

Valores válidos: una serie ASCII de una longitud máxima de 10 caracteres

Valor por omisión: nombre de cliente existente

nuevo-tipo-id

Indica el nuevo tipo de hardware del cliente.

Valores válidos: 0 - 21. Consulte la página 541.

Valor por omisión: tipo de hardware del cliente existente

nuevo-valor-id

Especifica el nuevo identificador de cliente.

Valores válidos: 0 ó cualquier dirección MAC válida (12 dígitos hexadecimales)

Valor por omisión: tipo de ID de cliente existente

Nota: Un **tipo-id** de 0 y un **valor-id** de 0 indica que el servidor no debe distribuir la dirección IP especificada.

nueva-dirección

Especifica la nueva dirección IP que se debe suministrar al cliente o una serie de caracteres que indica que no se dará

Mandatos de configuración de servidor DHCP (Talk 6)

servicio al cliente o que se puede suministrar al cliente con cualquier dirección de la agrupación de direcciones IP.

Valores válidos:

cualquier dirección IP válida

none Indica que no se dará servicio al cliente coincidente

any Indica que se puede suministrar al cliente cualquier dirección IP de la agrupación de subred.

Valor por omisión: ninguno

Nota: Un **tipo-id** de 0 y un **valor-id** de 0 indica que el servidor no debe distribuir la dirección IP especificada.

Ejemplo:

```
DHCP Server config> change client global
Enter the client name []? ClientA
Enter the new client name [ClientA]?
Enter the new client hardware type (0 - 21) [0]?
Enter the new client ID [ClientA]?
Enter the client's new IP address (IP address, any, none) [9.1.1.1]?
Client ClientA has been changed
```

Ejemplo:

```
DHCP Server config> change client subnet
Enter the subnet name []? subA
Enter the client name []? Clia
Enter the new client name [ClientA]?
Enter the new client hardware type (0 - 21) [1]?
Enter the new client ID [400000000010]?
Enter the client's new IP address (IP address, any, none) [10.1.1.10]?
Client Clia has been changed
```

subnet *nombre_subred nuevo_nombre_subred nueva_dirección_subred
nueva_máscara_subred nuevo_inicio_rango nuevo_fin_rango*
Modifica una subred.

nombre_subred

Indica el nombre de la subred específica que se va a modificar.

Valores válidos: un nombre de subred existente

Valor por omisión: ninguno

nuevo_nombre_subred

Indica el nuevo nombre de la subred especificada.

Valores válidos: cualquier serie ASCII de 10 caracteres

Valor por omisión: nombre de subred original

nueva_dirección_subred

Especifica la nueva dirección de la subred. La dirección se especifica en notación decimal punteada.

Valores válidos: cualquier dirección de subred IP válida

Valor por omisión: dirección de subred existente

Mandatos de configuración de servidor DHCP (Talk 6)

nueva_máscara_subred

Especifica la nueva máscara de dirección de subred. La dirección de subred debe estar en la máscara de subred y no puede contener un número de bits mayor que el de la máscara.

Valores válidos: cualquier máscara IP válida

Valor por omisión: máscara de subred existente

nuevo_inicio_rango

Especifica la nueva dirección IP inicial de la agrupación de direcciones IP que este servidor administrará para esta subred. Si no se especifica *inicio_rango*, el servidor administrará todas las direcciones de la subred.

Valores válidos: cualquier dirección IP válida dentro del rango de subred

Valor por omisión: Dirección inicial de agrupación existente

nuevo_fin_rango

Especifica la nueva dirección IP final de la agrupación de direcciones IP que este servidor administrará para esta subred.

Valores válidos: cualquier dirección IP válida dentro del rango de subred y mayor que la dirección de agrupación inicial

Valor por omisión: dirección final de agrupación existente

Ejemplo:

```
DHCP Server config> change subnet
Enter the subnet name []? subA
Enter the new subnet name [subA]?
Enter the new IP subnet [10.1.1.0]?
Enter the new IP subnet mask [255.255.0.0]?
Enter new start of IP address range [10.1.1.1]?
Enter new end of IP address range [10.1.1.31]?
Enter the new subnet group name [group11]?
Enter the new subnet group priority [1]?
Enter the new access policy list (Inorder or Balance) [Inorder]?
```

vendor-option *nombre_proveedor nuevo_nombre_proveedor [nuevo_valor_hex]*

Modifica una opción de proveedor.

nombre_proveedor

Especifica el nuevo nombre de la opción de proveedor.

Valores válidos: un nombre de proveedor existente

Valor por omisión: ninguno

nuevo_nombre_proveedor

Especifica el nuevo nombre de la opción de proveedor.

Valores válidos: una serie ASCII de una longitud máxima de 40 caracteres

Valor por omisión: nombre de opción de proveedor existente

nuevo_valor_hex

Especifica la nueva serie ASCII hexadecimal que representa el valor hexadecimal de la parte de datos de la opción. No se puede añadir un valor hexadecimal si se han añadido opciones específicas a esta opción de proveedor.

Valores válidos: cualquier serie hexadecimal válida

Valor por omisión: una serie hexadecimal existente

Ejemplo:

```
DHCP Server config> change vendor-option
Enter the vendor name []? XA-clients
Enter the new vendor name [XA-clients]?
Enter the new vendor data [01 aa 04]?
```

Delete

Utilice el mandato **delete** para suprimir una clase, un cliente, una opción, una subred, un grupo de subredes o una opción de proveedor.

Sintaxis:

```
delete          class
                  client
                  option
                  subnet
                  subnet-group
                  vendor-option
```

class *ámbito* [*nombre-subred*] *nombre-clase*

Suprime una clase y todas las opciones definidas bajo su ámbito.

ámbito Especifica el ámbito en el que se suprime la clase.

Valores válidos: global o subnet

Valor por omisión: ninguno

nombre-subred

Sólo es válido si el valor de **ámbito** es *subnet*. Especifica el nombre de la subred de la que se suprime la clase.

Valores válidos: cualquier nombre de subred existente

Valor por omisión: ninguno

nombre-clase

Indica el nombre de la clase que se va a suprimir.

Valores válidos: cualquier nombre de clase existente

Valor por omisión: ninguno

Mandatos de configuración de servidor DHCP (Talk 6)

Ejemplo:

```
DHCP Server config> delete class global
Enter the class name []? ClassA
```

Ejemplo:

```
DHCP Server config> delete class subnet
Enter the subnet name []? subA
Enter the class name []? ClaA
```

client *ámbito* [*nombre_subred*] *nombre_cliente*

Suprime un cliente y todas las opciones definidas bajo su ámbito.

ámbito Especifica el ámbito en el que se suprime el cliente.

Valores válidos: global o subnet

Valor por omisión: ninguno

nombre_subred

Sólo es válido si el valor de **ámbito** es *subnet*. Especifica el nombre de la subred de la que se suprime el cliente.

Valores válidos: un nombre de subred existente

Valor por omisión: ninguno

nombre_cliente

Indica el nombre del cliente que se va a suprimir.

Valores válidos: un nombre de cliente existente

Valor por omisión: ninguno

Ejemplo:

```
DHCP Server config> delete client global
Enter the client name []? ClientA
```

Ejemplo:

```
DHCP Server config> delete client subnet
Enter the subnet name []? subA
Enter the client name []? CliA
```

option *ámbito* [*nombre_subred*] [*nombre_clase*] [*nombre_cliente*]
[*nombre_proveedor*] *código*

Suprime una opción en el ámbito especificado.

ámbito Especifica el ámbito en el que se suprime la opción.

Valores válidos:

- class-global
- class-subnet
- client-global
- client subnet
- global
- subnet
- vendor-option

Valor por omisión: ninguno

nombre-subred

Sólo es válido si el valor de **ámbito** es *subnet*, *class-subnet* o *client-subnet*. Indica el nombre de la subred de la que se suprime el cliente.

Valores válidos: cualquier nombre de subred existente

Valor por omisión: ninguno

nombre-clase

Sólo es válido si el valor de **ámbito** es *class-global* o *class-subnet*. Indica el nombre de la clase de la que se suprime la opción.

Valores válidos: cualquier nombre de clase existente

Valor por omisión: ninguno

nombre-cliente

Sólo es válido si el valor de **ámbito** es *client-global* o *client-subnet*. Indica el nombre del cliente del que se suprime la opción.

Valores válidos: cualquier nombre de cliente existente

Valor por omisión: ninguno

nombre-proveedor

Sólo es válido si el valor de **ámbito** es *vendor-option*. Indica el nombre del proveedor del que se suprime la opción.

Valores válidos: cualquier nombre de proveedor existente

Valor por omisión: ninguno

código

Especifica el código de opción. Las opciones de DHCP están definidas en el documento RFC 2132. Consulte "Opciones de DHCP" en la página 515 para ver una descripción de las opciones y sus formatos.

Valores válidos: 1 - 255

Valor por omisión: 1

Mandatos de configuración de servidor DHCP (Talk 6)

Ejemplo:

```
DHCP Server config> delete option global
Enter the option code [1]? 3
```

Ejemplo:

```
DHCP Server config> delete option subnet
Enter the subnet name []? subA
Enter the option code [1]? 3
```

Ejemplo:

```
DHCP Server config> delete option class-global
Enter the class name []? ClassA
Enter the option code [1]? 3
```

Ejemplo:

```
DHCP Server config> delete option client
Enter the client name []? ClientA
Enter the option code [1]? 3
```

Ejemplo:

```
DHCP Server config> delete option class-subnet
Enter the subnet name []? subA
Enter the class name []? ClaA
Enter the option code [1]? 3
```

Ejemplo:

```
DHCP Server config> delete option client-subnet
Enter the subnet name []? subA
Enter the client name []? CliA
Enter the option code [1]? 3
```

Ejemplo:

```
DHCP Server config> delete option vendor-option
Enter the vendor name []? XI-clients
Enter the option code [1]? 85
```

Ejemplo:

```
DHCP Server config> delete option vendor-option
Enter the vendor name []? 200
Enter the option code [1]? 86
```

subnet *nombre_subred*

Suprime una subred y todas las clases, clientes y opciones definidos bajo su ámbito.

nombre_subred

Especifica el nombre de la subred que se suprime.

Valores válidos: cualquier nombre de subred existente

Valor por omisión: ninguno

Ejemplo:

```
DHCP Server config> delete subnet
Enter the subnet name []? subA
You are about to delete a subnet subA
and all the associated class, client, and option records associated with it
Are you sure you want to continue? [No]:
```

subnet-group *nombre_grupo_subredes*

Suprime todas las subredes asociadas a un grupo de subredes específicas y todas las clases, clientes y opciones definidos bajo los ámbitos de las subredes.

nombre_grupo_subredes

Especifica el nombre que identifica el grupo de subredes.

Valores válidos: un nombre de grupo de subredes existente

Valor por omisión: ninguno

Ejemplo:

```
DHCP Server config> delete subnet-group
Enter the subnet group name []? group2
You are about to delete a all subnets in group group2
and all the associated class, client, and option records associated with them
Are you sure you want to continue? [No]:
```

vendor-option *nombre_proveedor*

Suprime una opción de proveedor y las opciones definidas bajo su ámbito.

nombre_proveedor

Especifica el nombre del proveedor.

Valores válidos: una serie ASCII de una longitud máxima de 40 caracteres

Valor por omisión: ninguno

Ejemplo:

```
DHCP Server config> delete vendor-option
Enter the vendor name []? XA-clients
```

Disable

Utilice el mandato **disable** para inhabilitar globalmente el servidor DHCP.

Sintaxis:

```
disable          dhcp-server
```

Ejemplo:

```
DHCP Server config> disable dhcp-server
```

Enable

Utilice el mandato **enable** para habilitar globalmente el servidor DHCP.

Sintaxis:

```
enable          dhcp-server
```

Ejemplo:

```
DHCP Server config> enable dhcp-server
```

List

Utilice el mandato **list** para listar información de configuración acerca de una clase, un cliente, parámetros globales, subredes u opciones de proveedor y cualquier opción asociada.

Sintaxis:

```
list          class  
              client  
              global  
              option  
              subnet  
              vendor-option
```

```
class    all  
          global nombre-clase  
          subnet nombre-clase
```

Lista un resumen de todas las clases configuradas o los detalles de una clase específica.

nombre-clase

Indica el nombre de la clase que se va a visualizar.

Valores válidos: cualquier nombre de clase existente

Valor por omisión: ninguno

Ejemplo:

DHCP Server config> **list class all**

```

class          attached
name          to subnet
-----
ClassA
ClaA          subA

```

Ejemplo:

DHCP Server config> **list class global**

Enter the class name []? **ClassA**

```

class
name
-----
ClassA
Bootstrap Server: 100.100.100.100
Canonical: Yes
Support Unlisted Clients: Yes
Number of Options: 1
option  option
code    data
-----
1       255.255.0.0

```

Ejemplo:

DHCP Server config> **list class subnet**

Enter the subnet name []? **subA**

Enter the class name []? **ClaA**

```

class
name
-----
ClaA
starting IP address: 10.1.1.3
ending IP address: 10.1.1.5
Bootstrap Server: 100.100.100.100
Canonical: Yes
Support Unlisted Clients: DHCP

Number of Options: 1
option  option
code    data
-----
6       9.67.100.1

```

```

client    all
            global nombre-cliente
            subnet nombre-cliente

```

Lista un resumen de todos los clientes configurados o los detalles de un cliente específico.

nombre-cliente

Indica el nombre del cliente que se va a visualizar.

Valores válidos: un nombre de cliente existente

Mandatos de configuración de servidor DHCP (Talk 6)

Valor por omisión: ninguno

Ejemplo:

```
DHCP Server config> list client all
client  client  client  attached  IP
name    type    identifier  to subnet  address
-----
ClientA  0      ClientA
          9.1.1.1

CliA    1      400000000010  subA      10.1.1.10
```

Ejemplo:

```
DHCP Server config> list client global
Enter the client name []? ClientA
```

Ejemplo:

```
DHCP Server config> list client subnet
Enter the subnet name []? subA
Enter the client name []? CliA

client  client  client  IP
name    type    identifier  address
-----
CliA    1      400000000010  10.1.1.10
Bootstrap Server: 200.200.200.200
Canonical: Yes

Number of Options: 1
option  option
code    data
-----
6       9.67.100.1
```

global

Lista parámetros globales.

Ejemplo:

```
DHCP Server config> list global

DHCP server Global Parameters
=====
DHCP server enabled: Yes

Balance: group2

Inorder: group1

Canonical: No

Lease Expire Interval: 1 minute(s)
Lease Time Default: 1 day(s)

Support BOOTP Clients: No
Bootstrap Server: Not configured

Support Unlisted Clients: Yes
Ping Time: 1 second(s)
Used IP Address Expire Interval: 15 minute(s)
```

option *ámbito* [*nombre-subred*] [*nombre-clase*] [*nombre-cliente*] [*nombre-proveedor*]
código

ámbito Especifica el ámbito en el que se lista la opción.

Valores válidos:

- class-global
- class-subnet
- client-global
- client subnet
- global
- subnet
- vendor-option

Valor por omisión: ninguno

nombre-subred

Sólo es válido si el valor de **ámbito** es *subnet*, *class-subnet* o *client-subnet*. Indica el nombre de la subred a la que pertenece la opción listada.

Valores válidos: cualquier nombre de subred existente

Valor por omisión: ninguno

nombre-clase

Sólo es válido si el valor de **ámbito** es *class-global* o *class-subnet*. Indica el nombre de la clase a la que pertenece la opción listada.

Valores válidos: cualquier nombre de clase existente

Valor por omisión: ninguno

nombre-cliente

Sólo es válido si el valor de **ámbito** es *client-global* o *client-subnet*. Indica el nombre del cliente al que pertenece la opción listada.

Valores válidos: cualquier nombre de cliente existente

Valor por omisión: ninguno

nombre-proveedor

Sólo es válido si el valor de **ámbito** es *vendor-option*. Indica el nombre del proveedor al que pertenece la opción listada.

Valores válidos: cualquier nombre de proveedor existente

Valor por omisión: ninguno

código

Especifica el código de opción. Las opciones de DHCP están definidas en el documento RFC 2132. Consulte "Opciones de DHCP" en la página 515 para ver una descripción de las opciones y sus formatos.

Valores válidos: 1 - 255

Valor por omisión: 1

Mandatos de configuración de servidor DHCP (Talk 6)

Ejemplo:

```
DHCP Server config> list option global
```

```
option  option
code    data
-----
3       9.67.100.1
```

Ejemplo:

```
DHCP Server config> list option class-global
```

```
Enter the class name []? ClassA
```

```
option  option
code    data
-----
```

```
3       9.67.100.1
```

Ejemplo:

```
DHCP Server config> list option class-subnet
```

```
Enter the subnet name []? subA
```

```
Enter the class name []? claA
```

```
option  option
code    data
-----
```

```
3       9.67.100.1
```

Ejemplo:

```
DHCP Server config> list option client-global
```

```
Enter the client name []? ClientA
```

```
option  option
code    data
-----
```

```
3       9.67.100.1
```

Ejemplo:

```
DHCP Server config> list option client-subnet
```

```
Enter the subnet name []? subA
```

```
Enter the client name []? cliA
```

```
option  option
code    data
-----
```

```
3       9.67.100.1
```

Ejemplo:

```
DHCP Server config> list option subnet
```

```
Enter the subnet name []? subA
```

```
option  option
code    data
-----
6       9.67.100.1
```

Ejemplo:

```
DHCP Server config> list option vendor-option
Enter the vendor name []? XI-clients
```

```
option  option
code    data
-----
85      hex:01 aa 04
86      9.67.85.4
```

```
subnet  all
          detailed nombre-subred
```

Lista un resumen de todas las subredes configuradas o los detalles de una subred específica.

nombre-subred

Indica el nombre de la subred que se va a visualizar.

Valores válidos: un nombre de subred existente

Valor por omisión: ninguno

Mandatos de configuración de servidor DHCP (Talk 6)

Ejemplo:

DHCP Server config> **list subnet all**

name	address	mask	IP Addr	IP Addr
subA	10.1.1.0	255.255.0.0	10.1.1.1	10.1.1.31
subB	11.1.1.0	255.255.0.0	11.1.1.1	11.1.1.31

Ejemplo:

DHCP Server config> **list subnet detailed**

Enter the subnet name []? **subA**

subnet name	subnet address	subnet mask	starting IP Addr	ending IP Addr
subA	10.1.1.0	255.255.0.0	10.1.1.1	10.1.1.31

Subnet Group: group1/1

Number of Classes: 1

class

name

ClaA

starting IP address: 10.1.1.1

ending IP address: 10.1.1.6

Bootstrap Server: 100.100.100.100

Canonical: Yes

Support Unlisted Clients: DHCP

Number of Options: 1

option option

code data

6 9.67.100.1

Number of Clients: 1

client name	client type	client identifier	IP address
-------------	-------------	-------------------	------------

CliA	1	400000000010	10.1.1.10
------	---	--------------	-----------

Bootstrap Server: 200.200.200.200

Canonical: Yes

Number of Options: 1

option option

code data

6 9.67.100.1

Number of Options: 1

option option

code data

1 255.255.255.0

vendor-option

all

detailed nombre-proveedor

Lista un resumen de todos los proveedores configurados o los detalles de una opción de proveedor específica.

nombre-proveedor

Indica el nombre de la opción de proveedor que se va a visualizar.

Valores válidos: un nombre de proveedor existente

Valor por omisión: ninguno

Ejemplo:

```
DHCP Server config> list vendor-option all
```

```

vendor      hex
name        data
-----
XA-clients  01 AA 04
XI-clients

```

```
DHCP Server config> list vendor-option detailed
```

```

Enter the vendor name []? XI-clients
vendor      hex
name        data
-----
XI-clients

Number of Options: 2
option      option
code        data
-----
85          hex:01 AA 04
86          9.67.85.4

```

Set

Utilice el mandato **set** para especificar valores para parámetros globales y añadir grupos de subredes a las listas Balance e Inorder.

Sintaxis:

```

set          balance
            bootstrapserver
            canonical
            inorder
            lease-expire-interval
            lease-time-default
            ping-time
            support-bootp
            support-unlisted-clients
            used-ip-address-expire-interval

```

balance *nombre_grupo_subredes*

Añade o mueve un grupo de subredes a la lista Balance. Las direcciones se asignarán de manera rotatoria desde todas las subredes asociadas con el grupo o grupos definido(s) en un grupo de subredes, según su prioridad.

Mandatos de configuración de servidor DHCP (Talk 6)

nombre_grupo_subredes

Especifica el nombre del grupo de subredes al que pertenece esta subred.

Valores válidos: un nombre de grupo de subredes existente

Valor por omisión: ninguno

Ejemplo:

```
DHCP Server config> set balance
Enter the subnet group name []? group1
```

bootstrapsver *ámbito* [*nombre-subred*] [*nombre-clase*] [*nombre-cliente*] *dirección*

Especifica si el servidor DHCP indica o no un servidor de rutina de carga para clientes. Si desea que el servidor DHCP especifique un servidor de rutina de carga, debe definir la dirección IP del servidor. Este parámetro puede especificarse en el ámbito global, de subred, de clase o de cliente.

ámbito Especifica el ámbito del parámetro bootstrapsver.

Valores válidos:

- class-global
- class-subnet
- client-global
- client-subnet
- global
- subnet

Valor por omisión: ninguno

nombre-subred

Es válido si el ámbito es *subnet*, *class-subnet* o *client-subnet*. Indica el nombre de la subred para la que se especifica el servidor de rutina de carga.

Valores válidos: un nombre de subred existente

Valor por omisión: ninguno

nombre-clase

Es válido si el ámbito es *class-global* o *class-subnet*. Indica el nombre de la clase para la que se especifica el servidor de rutina de carga.

Valores válidos: cualquier nombre de clase existente

Valor por omisión: ninguno

nombre-cliente

Es válido si el ámbito es *client-global* o *client-subnet*. Indica el nombre del cliente para el que se especifica el servidor de rutina de carga.

Valores válidos: un nombre de cliente existente

Valor por omisión: ninguno

dirección IP del servidor

Especifica la dirección IP del servidor de rutina de carga.

Valores válidos: cualquier dirección IP válida en formato decimal con puntos

Valor por omisión: ninguno

Ejemplo:

```
DHCP Server config> set bootstrap-server class-global
Enter the class name []? ClassA
Enter the IP address of the server []? 100.100.100.100
```

Ejemplo:

```
DHCP Server config> set bootstrap-server class-subnet
Enter the subnet name []? subA
Enter the class name []? ClassA
Enter the IP address of the server []? 100.100.100.100
```

Ejemplo:

```
DHCP Server config> set bootstrap-server client-global
Enter the client name []? ClientA
Enter the IP address of the server []? 100.100.100.100
```

Ejemplo:

```
DHCP Server config> set bootstrap-server client-subnet
Enter the subnet name []? subA
Enter the client name []? ClientA
Enter the IP address of the server []? 100.100.100.100
```

Ejemplo:

```
DHCP Server config> set bootstrap-server global
Enter the IP address of the server []? 100.100.100.100
```

Ejemplo:

```
DHCP Server config> set bootstrap-server subnet
Enter the subnet name []? subA
Enter the IP address of the server []? 100.100.100.100
```

canonical *ámbito [nombre-subred] [nombre-clase] [nombre-cliente] valor*

Especifica si el servidor DHCP transformará las direcciones MAC al formato canónico.

Las direcciones MAC para los clientes Ethernet/802.3 se almacenan en el formato canónico (el byte empieza con el bit menos significativo). Las direcciones MAC para los clientes Token-Ring se almacenan en el formato no canónico (el byte empieza con el bit más significativo). Este parámetro debe utilizarse cuando el servidor DHCP esté en un tipo de medio (Token-Ring o Ethernet/802.3), el cliente esté en el otro tipo de medio y exista un puente de conversión entre ambos. Cuando este parámetro se define como *yes*, el servidor DHCP hará que la dirección MAC del cliente alterne del formato canónico al no canónico, o del no canónico al canónico. Dado que el servidor DHCP no sabe en qué formato estaba originalmente la dirección MAC, la definición de este parámetro como *yes* sólo alternará la dirección. El formato canónico se puede definir en el ámbito global, de subred, de clase o de cliente.

Mandatos de configuración de servidor DHCP (Talk 6)

ámbito	<p>Especifica el ámbito del parámetro bootstrapsver.</p> <p>Valores válidos:</p> <ul style="list-style-type: none">• class-global• class-subnet• client-global• client-subnet• global• subnet <p>Valor por omisión: ninguno</p>
nombre-subred	<p>Es válido si el ámbito es <i>subnet</i>, <i>class-subnet</i> o <i>client-subnet</i>. Indica el nombre de la subred para la que se especifica el formato canónico.</p> <p>Valores válidos: un nombre de subred existente</p> <p>Valor por omisión: ninguno</p>
nombre-clase	<p>Es válido si el ámbito es <i>class-global</i> o <i>class-subnet</i>. Indica el nombre de la clase para la que se especifica el formato canónico.</p> <p>Valores válidos: cualquier nombre de clase existente</p> <p>Valor por omisión: ninguno</p>
nombre-cliente	<p>Es válido si el ámbito es <i>client-global</i> o <i>client-subnet</i>. Indica el nombre del cliente para el que se especifica el formato canónico.</p> <p>Valores válidos: un nombre de cliente existente</p> <p>Valor por omisión: ninguno</p>
valor	<p>Especifica si las direcciones MAC van a transformarse al formato canónico</p> <p>Valores válidos: yes, no</p> <p>Valor por omisión: no, si el valor de ámbito es <i>global</i>. De lo contrario, el valor por omisión se determina mediante la jerarquía de ámbitos. Consulte “Conceptos y terminología” en la página 512 para obtener una explicación del ámbito.</p>

Mandatos de configuración de servidor DHCP (Talk 6)

Ejemplo:

```
DHCP Server config> set canonical class-global
Enter the class name []? ClassA
Would you like MAC addresses to be transformed to canonical format? [No] yes
```

Ejemplo:

```
DHCP Server config> set canonical class-subnet
Enter the subnet name []? subA
Enter the class name []? ClassA
Would you like MAC addresses to be transformed to canonical format? [No] yes
```

Ejemplo:

```
DHCP Server config> set canonical client-global
Enter the client name []? ClientA
Would you like MAC addresses to be transformed to canonical format? [No] yes
```

Ejemplo:

```
DHCP Server config> set canonical client-subnet
Enter the subnet name []? subA
Enter the client name []? ClientA
Would you like MAC addresses to be transformed to canonical format? [No] yes
```

Ejemplo:

```
DHCP Server config> set canonical global
Would you like MAC addresses to be transformed to canonical format? [No] yes
```

Ejemplo:

```
DHCP Server config> set canonical subnet
Enter the subnet name []? subA
Would you like MAC addresses to be transformed to canonical format? [No] yes
```

inorder *lista-etiquetas*

Añade o mueve un grupo de subredes a la lista Inorder. Las direcciones se asignarán desde las subredes de un grupo de subredes, en el orden de prioridad asignado a esta subred.

nombre_grupo_subredes

Especifica el grupo de subredes al que pertenece esta subred.

Valores válidos: un nombre de grupo de subredes existente

Valor por omisión: ninguno

Ejemplo:

```
DHCP Server config> set inorder
Enter the subnet group name []? g2
```

lease-expire-interval *tiempo longitud*

Especifica el intervalo al que se examina la condición de alquiler de todas las direcciones de la agrupación de direcciones, para determinar qué alquileres han caducado. El intervalo de caducidad de alquiler sólo se puede definir a nivel global.

tiempo Especifica la unidad de medida del tiempo.

Valores válidos: segundos, minutos, horas

Valor por omisión: ninguno

Mandatos de configuración de servidor DHCP (Talk 6)

longitud Especifica la longitud del intervalo.

Valores válidos: 15 segundos - 12 horas

Valor por omisión:

- 15 (si la unidad de tiempo es el segundo)
- 1 (si la unidad de tiempo es el minuto)
- 1 (si la unidad de tiempo es la hora)

Ejemplo:

```
DHCP Server config> set lease-expire-interval seconds
How long is the interval in seconds (max:59) [15]? 59
```

Ejemplo:

```
DHCP Server config> set lease-expire-interval minutes
How long is the interval in minutes (max:59) [1]? 45
```

Ejemplo:

```
DHCP Server config> set lease-expire-interval hours
How long is the interval in hours (max:12) [1]? 2
```

lease-time-default *tiempo longitud*

Especifica la duración del alquiler por omisión para los alquileres emitidos por el servidor DHCP. Un intervalo infinito significa que los alquileres no caducarán nunca. El valor por omisión del tiempo de alquiler sólo se puede definir a nivel global.

tiempo Especifica la unidad de medida del tiempo.

Valores válidos: minutos, horas, días, semanas, meses, años, infinito

Valor por omisión: ninguno

longitud Especifica la longitud del intervalo.

Valores válidos: 3 minutos - infinito

Valor por omisión:

- 3 (si la unidad de tiempo es el minuto)
- 1 (si la unidad de tiempo es la hora)
- 1 (si la unidad de tiempo es el día)
- 1 (si la unidad de tiempo es el mes)
- 1 (si la unidad de tiempo es el año)

Mandatos de configuración de servidor DHCP (Talk 6)

Ejemplo:

```
DHCP Server config> set lease-time-default minutes
How long is the interval in minutes (max:59) [3]? 2
```

Ejemplo:

```
DHCP Server config> set lease-time-default hours
How long is the interval in hours (max:23) [1]? 45
```

Ejemplo:

```
DHCP Server config> set lease-time-default days
How long is the interval in days (max:6) [1]? 2
```

Ejemplo:

```
DHCP Server config> set lease-time-default weeks
How long is the interval in weeks (max:3) [1]? 1
```

Ejemplo:

```
DHCP Server config> set lease-time-default months
How long is the interval in months (max:11) [1]? 3
```

Ejemplo:

```
DHCP Server config> set lease-time-default years
How long is the interval in years (max:10) [1]? 3
```

Ejemplo:

```
DHCP Server config> set lease-time-default infinity
```

ping-time *tiempo longitud*

Antes de asignar una dirección IP, el servidor DHCP realiza una prueba para asegurarse de que no se está utilizando la dirección IP. Este valor especifica cuánto tiempo esperará el servidor DHCP una respuesta PING antes de marcar la dirección como disponible. El valor 0 inhabilita los PING, lo que da como resultado que el servidor DHCP no prueba una dirección antes de asignarla.

tiempo Especifica la unidad de medida del tiempo.

Valores válidos: segundos

Valor por omisión: ninguno

longitud Especifica la longitud del intervalo.

Valores válidos: 0 - 5 segundos

Valor por omisión: 1

Ejemplo:

```
DHCP Server config> set ping-time seconds
How long is the interval in seconds (max:5) [1]? 10
```

support-bootp *valor*

Especifica si el servidor responderá a las peticiones de los clientes BOOTP. Si el servidor DHCP se configuró anteriormente para dar soporte a clientes BOOTP y se ha vuelto a configurar para no dar soporte a los clientes BOOTP, el vínculo de dirección para cualquier cliente BOOTP establecido antes de la reconfiguración, se mantendrá

Mandatos de configuración de servidor DHCP (Talk 6)

hasta que el cliente BOOTP envíe otra petición (cuando se reinicie). En ese momento, el servidor no responderá y el vínculo será eliminado. Este parámetro sólo se puede definir a nivel global.

Valores válidos: yes o no

Valor por omisión: no

Ejemplo:

```
DHCP Server config> set support-bootp
Would you like the server to support BOOTP clients? [No] 10
```

support-unlisted-clients *ámbito [nombre-subred] [nombre-clase] valor*

Especifica si el servidor responderá a las peticiones de los clientes DHCP distintos de aquéllos cuyos ID de cliente están listados específicamente en esta configuración. Este parámetro tiene varios valores posibles:

ámbito Especifica el ámbito del parámetro **support-unlisted-clients**.

Valores válidos:

- class-global
- class-subnet
- global
- subnet

Valor por omisión: ninguno

nombre-subred

Es válido si el valor de ámbito es *subnet*, *class-subnet* o *client-subnet*. Indica el nombre de la subred para la que se especifica este parámetro.

Valores válidos: un nombre de subred existente

Valor por omisión: ninguno

nombre-clase

Es válido si el valor de ámbito es *class-global* o *class-subnet*. Indica el nombre de la clase para la que se especifica este parámetro.

Valores válidos: cualquier nombre de clase existente

Valor por omisión: ninguno

valor

yes El servidor DHCP debe responder a cualquier cliente, no importa el tipo ni si está configurado.

no El servidor DHCP sólo responderá a las peticiones de los clientes DHCP que están configurados.

bootp El servidor DHCP dará soporte a los clientes BOOTP no listados, pero no a los clientes DHCP no listados

Mandatos de configuración de servidor DHCP (Talk 6)

dhcp El servidor DHCP responderá a los clientes DHCP no listados, pero no a los clientes BOOTP no listados.

Valores válidos: yes, no, bootp, dhcp

Valor por omisión: yes, si **ámbito** es *global*. De lo contrario, el valor por omisión se determina mediante la jerarquía de ámbitos. Consulte “Conceptos y terminología” en la página 512 para obtener una explicación del ámbito.

Ejemplo:

```
DHCP Server config> set support-unlisted-clients class-global yes
Enter the class name []? ClassA
```

Ejemplo:

```
DHCP Server config> set support-unlisted-clients class-subnet no
Enter the subnet name []? subA
Enter the class name []? ClassA
```

Ejemplo:

```
DHCP Server config> set support-unlisted-clients global bootp
```

Ejemplo:

```
DHCP Server config> set support-unlisted-clients subnet dhcp
Enter the subnet name []? subA
```

used-ip-address-expire-interval *tiempo longitud*

Especifica el intervalo que el servidor retendrá una dirección IP en uso, antes de que la dirección quede disponible para su asignación. Antes de que el servidor asigne una dirección IP, realiza PING en la dirección para asegurarse de que no se está utilizando ya en la red. Entonces, el servidor marca la dirección en uso que está reservada. Este parámetro especifica cuánto tiempo se mantiene reservada una dirección en uso, antes de designar la dirección como disponible para su asignación. Este parámetro sólo se puede definir a nivel global.

tiempo Especifica la unidad de medida del tiempo.

Valores válidos: segundos, minutos, horas, días, semanas, meses, años, infinito

Valor por omisión: ninguno

longitud Especifica la longitud del intervalo.

Valores válidos: 30 segundos - infinito

Valor por omisión:

- 30 (si la unidad de tiempo es el segundo)
- 15 (si la unidad de tiempo es el minuto)
- 1 (si la unidad de tiempo es la hora)
- 1 (si la unidad de tiempo es el día)
- 1 (si la unidad de tiempo es el mes)
- 1 (si la unidad de tiempo es el año)

Ejemplo:

```
DHCP Server config> set used-ip-address-expire-interval seconds
How long is the interval in seconds (max:59) [30]? 2
```

Ejemplo:

```
DHCP Server config> set used-ip-address-expire-interval minutes
How long is the interval in minutes (max:59) [15]? 2
```

Ejemplo:

```
DHCP Server config> set used-ip-address-expire-interval hours
How long is the interval in hours (max:23) [1]? 5
```

Ejemplo:

```
DHCP Server config> set used-ip-address-expire-interval days
How long is the interval in days (max:6) [1]? 2
```

Ejemplo:

```
DHCP Server config> set used-ip-address-expire-interval weeks
How long is the interval in weeks (max:3) [1]? 1
```

Ejemplo:

```
DHCP Server config> set used-ip-address-expire-interval months
How long is the interval in months (max:11) [1]? 3
```

Ejemplo:

```
DHCP Server config> set used-ip-address-expire-interval years
How long is the interval in years (max:10) [1]? 3
```

Ejemplo:

```
DHCP Server config> set used-ip-address-expire-interval infinity
```

Acceso al entorno de supervisión de servidor DHCP

Utilice el siguiente procedimiento para acceder al proceso de *supervisión* del servidor DHCP.

1. En el indicador OPCON, entre **talk 5**. Por ejemplo:

```
* talk 5
Config>
```

Después de entrar el mandato **talk 5**, el indicador CONFIG (+) se visualiza en la terminal. Si el indicador no aparece al entrar la configuración por primera vez, pulse de nuevo **Return**.

2. En el indicador +, entre el mandato **feature dhcp-server** para acceder al indicador DHCP Server>.

Mandatos de supervisión del servidor DHCP

Tabla 63. Resumen de los mandatos de supervisión del servidor DHCP

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxiv.
Disable	Inhabilita dinámicamente el servidor DHCP.
Enable	Habilita dinámicamente el servidor DHCP.
List	Visualiza los parámetros globales y para clases, clientes, subredes y opciones de proveedor.
Reset	Restablece dinámicamente la configuración del servidor DHCP.
Request	
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiv.

Disable

Utilice el mandato **disable** para inhabilitar dinámicamente el servidor DHCP.

Sintaxis:

disable dhcp

Enable

Utilice el mandato **enable** para habilitar dinámicamente el servidor DHCP.

Sintaxis:

enable dhcp

List

Utilice el mandato **list** para listar información de configuración acerca de una clase, un cliente, parámetros globales, subredes, opción de proveedor y cualquier opción asociada. Consulte “List” en la página 556 para obtener ejemplos del mandato **list**.

Sintaxis:

list class
 client
 global
 option
 subnet
 vendor-option

Reset

Utilice el mandato **reset** para restablecer dinámicamente la configuración del servidor DHCP.

Sintaxis:

reset dhcp

Ejemplo:

```
DHCP Server> reset dhcp
You are about to reset the DHCP Server. Clients who have been granted a lease by this
server will need to renew it.
Are you sure you want to continue? [No]: y
DHCP Server has been reset
DHCP Server>
```

Request

Utilice el mandato **request** para visualizar la información de administración.

Sintaxis:

request clientid
 delete
 ipquery
 poolquery
 stats
 status

clientid *id_cliente*

Visualiza información para un cliente.

id_cliente

Indica el identificador del cliente.

Valores válidos: un ID de cliente existente

Valor por omisión: ninguno

Ejemplo:

```
DHCP Server> request clientid
Enter the client name []? 0020351FB371

Client id: 1-0x0020351FB371
Status: BOUND
Address last assigned: 192.9.200.10
Most recent lease time: 16:41:25 December 3, 1998
Proxy flag: FALSE
Hostname: Win-XY-1
Domain name: city.net
```

delete *dirección*

Suprime un alquiler para la dirección IP de un cliente específico.

dirección Indica la dirección IP del cliente que se va a suprimir.

Valores válidos: cualquier dirección IP válida de un cliente existente

Valor por omisión: ninguno

Ejemplo:

```
DHCP Server> request delete
Enter the client's IP address []? 194.3.200.10
```

ipquery *address*

Visualiza información para una dirección IP.

Ejemplo:

```
DHCP Server>req ipquery 192.168.8.3
IP address:      192.168.8.3
Status:          RECLAIMED
Lease time:      86400 seconds
Start time:      Not Leased
Last time leased: 04:16:33 March 9, 1999
DHCP Server>
```

poolquery *dirección*

Visualiza información para una agrupación de direcciones IP.

dirección Indica una dirección IP en la agrupación que se va a visualizar.

Valores válidos: cualquier dirección IP válida en la agrupación que se va a visualizar

Valor por omisión: ninguno

Ejemplo:

```
DHCP Server> request poolquery

Enter the client's IP address []? 194.3.200.10
IP address:      194.3.200.10
Status:          LEASED
Lease time:      86400 seconds
Start time:      16:41:25 December 3, 1998
Last time leased: 16:41:25 December 3, 1998
Client id:       1-0x0020351FB371
Hostname:        Win-XY-1
Domain name:     city.net
IP address:      194.3.200.11
Status:          STOCKED
IP address:      194.3.200.12
Status:          STOCKED
```

stats

Visualiza información estadística acerca de la agrupación de direcciones administrada por el servidor. Las estadísticas incluyen: paquetes de descubrimiento procesados, paquetes de descubrimiento sin respuesta, ofertas realizadas, alquileres otorgados, reconocimientos negativos (NAK), informes procesados, incluidos los informes más los reconocimientos (ACK), renovaciones, releases, clientes BOOTP procesados, intentos de actualización de proxyARec, paquetes no soportados.

Sintaxis: request stats

Mandatos de supervisión del servidor DHCP (Talk 6)

Ejemplo:

```
DHCP Server> request stats
Number of DISCOVER requests received:      8
Number of OFFER responses sent:            4
Number of ACK responses sent:              3
Number of NACK responses sent:             0
Number of RELEASE requests received:      0
Number of DECLINE packets received:       0
Number of INFORM requests received:       0
Number of BOOTP requests received:        0
Number of requests received via proxy:    0
Number of UNSUPPORTED requests received:  0
Total number of request/responses:        15
Number of lease expirations:              0
```

status Visualiza información acerca de las agrupaciones de direcciones.

Ejemplo:

```
DHCP Server> request status

IP address:      194.3.200.10
Status:          LEASED
Lease time:      86400 seconds
Start time:     16:41:25 December 3, 1998
Last time leased: 16:41:25 December 3, 1998
Client id:      1-0x0020351FB371
Hostname:       Win-XY-1
Domain name:    city.net

IP address:      194.3.200.11
Status:          STOCKED

IP address:      194.3.200.12
Status:          STOCKED

IP address:      194.3.200.10
Status:          STOCKED
```

Utilización de la característica Thin Server

Este capítulo describe cómo utilizar la característica Thin Server (TSF) en el IBM 2216.

Visión general de la Network Station

Una Network Station es similar a un sistema personal (PC), ya que tiene un teclado, una pantalla y un ratón. La diferencia principal entre una Network Station y un PC es que los archivos de la Network Station residen en un servidor de red, en vez de estar en una unidad de disco duro situada en el interior de la máquina. La Network Station le presenta una interfaz de usuario gráfica (GUI), que proporciona acceso a muchos recursos, incluidos los emuladores, aplicaciones X remotas, navegadores Web, aplicaciones e impresoras.

La Network Station se comunica con el servidor utilizando TCP/IP a través de una conexión Red en Anillo o Ethernet. El proceso de encendido de la Network Station es la siguiente:

- Se inicia un programa supervisor de arranque, residente en la memoria de acceso aleatorio no volátil, y se ejecutan las autopruebas de encendido.
- La Network Station establece contacto con un servidor BootP o DHCP, que proporciona información a la Network Station, como su dirección IP, su(s) dirección(es) de servidor y el nombre y la vía de acceso del archivo de arranque. Por otra parte, la Network Station puede recuperar esta información de los valores almacenados en su memoria de acceso aleatorio no volátil.
- La Network Station utiliza el protocolo TFTP (Trivial File Transfer Protocol), Remote File System/400 (RFS/400) o Network File System (NFS) para bajar el código base, como el sistema operativo, los archivos de configuración de hardware y los programas de aplicación del servidor de código base.
- La Network Station baja la información de configuración basada en la terminal, como la configuración para una impresora conectada a la Network Station o como el idioma del teclado de la Network Station, desde el servidor de configuración de terminal.
- La Network Station presenta una pantalla de inicio de sesión. Entonces puede entrar un ID de usuario y una contraseña.
- El servidor de autenticación valida el ID de usuario y la contraseña y le permite acceder a los archivos de usuario personales.
- Se bajan las preferencias del entorno personalizadas.
- La Network Station visualiza el escritorio personalizado.

Consulte el manual *IBM Network Station Manager Installation and Use*, SC41-0664, para obtener más información acerca de las Network Stations.

Visión general de la característica Thin Server

Un dispositivo físico puede funcionar como el servidor BootP/DHCP, el servidor de arranque, el servidor de configuración de terminal y el servidor de autenticación, o cada servidor puede ser un dispositivo distinto. Por ejemplo, puede tener una Network Station conectada a un AS/400, que actúa como servidor BootP, servidor de código base, servidor de configuración de terminal y servidor de autenticación. Por otra parte, cada servidor puede ser una caja física distinta. Por ejemplo, la Network Station puede estar conectada a una red en la que un servidor NT es su servidor DHCP, un AS/400 es su servidor de código base, otro AS/400 es su servidor de configuración de terminal y un tercer AS/400 es su servidor de autenticación.

La característica Thin Server permite que el 2216 sea un servidor de código base. Un ejemplo de la razón de que sea deseable utilizar el TSF está ilustrado en la Figura 46 en la página 579 y en la Figura 47 en la página 579. En la Figura 46 en la página 579, del único servidor se bajará cualquier archivo que la Network Station necesite. Cuando la Network Station esté encendida, esta operación de bajada consistirá en varios megabytes. Esto podría ser muy complicado en una infraestructura de red, así como el dispositivo que actúa como servidor de configuración de código base/terminal o como servidor de autenticación, sobre todo si se encienden muchas Network Stations simultáneamente. La Figura 47 en la página 579 muestra la red con un Thin Server utilizado en el sitio remoto. El Thin Server colocará en la antememoria muchos de los archivos asociados al código de arranque de la Network Station. Cuando se enciende la Network Station, la mayoría del código de arranque se carga desde el Thin Server y sólo una pequeña cantidad de datos tiene que ser transportada a través de la infraestructura de red. Este proceso reducido en cualquier servidor baja el tráfico de la red y reduce el tiempo necesario para completar el proceso de encendido de una Network Station.

Dado que los archivos que el Thin Server coloca en la antememoria son copias de los archivos que residen en el servidor de archivos maestro, cada vez que se modifica la versión que hay en el servidor de archivos maestro, el Thin Server tiene que actualizar su versión de ese archivo. El Thin Server verificará que todos los archivos en la antememoria son idénticos a la versión del servidor de archivos maestro de estos archivos cuando:

1. El IBM 2216 esté encendido
2. El IBM 2216 se vuelva a cargar o a iniciar
3. El TSF se reinicie
4. Se alcance el intervalo de tiempo especificado en la configuración de TSF
5. Un parámetro de acción SNMP MIB lo desencadene
6. Se emita el mandato TSF talk 5 **refresh**
7. Cada vez que se acceda a un archivo (excepto TFTP). El TSF verificará que cada archivo accedido coincida con la versión en el servidor de archivos maestro. Cuando se detecte una diferencia, se actualizará el archivo. A continuación, el TSF verificará que los archivos restantes coincidan también con la versión que hay en el servidor de archivos maestro.

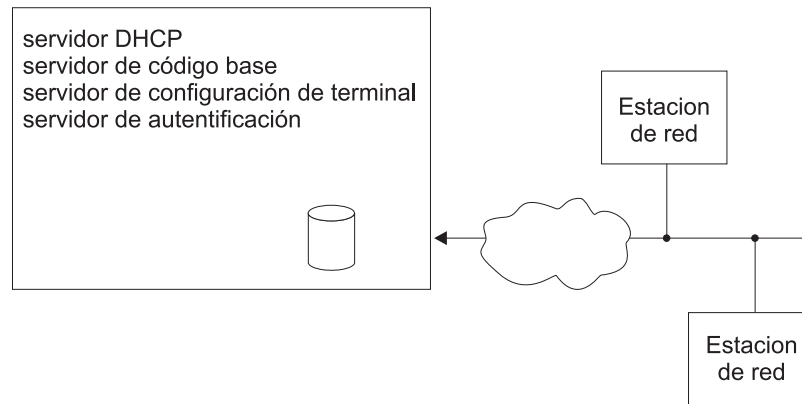


Figura 46. Network Station remota sin un Thin Server

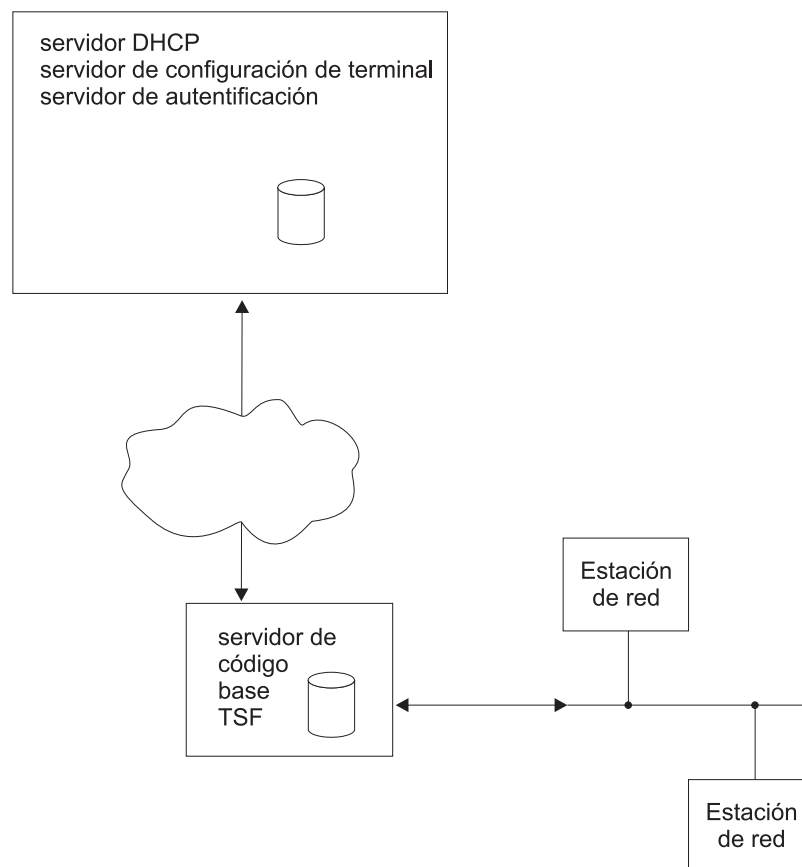


Figura 47. Network Station remota con un Thin Server

Soporte de BootP/DHCP

Tiene dos opciones para el soporte de Servidor BootP/DHCP:

- Utilice el soporte de servidor DHCP de IBM 2216. Consulte “Utilización del servidor DHCP” en la página 507.

Utilización de TSF

- Configure el IBM 2216 para que actúe como agente Relay para peticiones BootP/DHCP. Consulte el manual *Consulta de configuración y supervisión de protocolos Volumen 1* para obtener información adicional.

Consulte el manual *IBM Network Station Manager Installation and Use*, SC41-0664, para obtener más información acerca de varios entornos de servidor.

Protocolos utilizados para establecer comunicación con las Network Stations

Los protocolos utilizados para establecer comunicación entre la Network Station y sus servidores se determinará mediante la configuración de BootP/DHCP o mediante la configuración NVRAM de Network Station. En cualquier caso, los protocolos que Network Station utiliza deben ser compatibles con la manera como está configurado el TSF.

Si el TSF está configurado para utilizar RFS para establecer comunicación con el servidor de archivos maestro, aceptará las peticiones RFS y TFTP de las Network Stations, y el TSF no responderá a ninguna petición NFS de las Network Stations.

De manera similar, si el TSF está configurado para utilizar NFS para establecer comunicación con el servidor de archivos maestro, aceptará las peticiones NFS y TFTP de las Network Stations, y el TSF no responderá a ninguna petición RFS de las Network Stations.

Utilización de RFS

El TSF establece una conexión con el AS/400 utilizando RFS. Cuando una Network Station realiza una petición para abrir un archivo, el TSF reenviará esa petición al AS/400 para obtener autorización. Si la Network Station no está autorizada, el TSF no enviará el archivo solicitado a la Network Station. Si la Network Station está autorizada y la versión de AS/400 del archivo solicitado difiere de la versión almacenada en el TSF IBM 2216, la petición de la Network Station se transmitirá al AS/400. Si el archivo en el AS/400 es la misma versión que el archivo que el TSF ha colocado en la antememoria, el TSF servirá ese archivo a la Network Station.

Si la conexión del TSF al AS/400 no está disponible, el TSF servirá a la Network Station los archivos que ha colocado en la antememoria.

Utilización de TFTP

Si se utiliza TFTP para establecer comunicación entre la Network Station y el TSF, el TSF servirá las peticiones de archivos de la Network Station si estos archivos están disponibles. No se realiza ninguna verificación de versión entre el TSF y el servidor de archivos maestro. Si el archivo no está disponible en la antememoria de TSF, la petición de la Network Station se reenvía al servidor de archivos maestro.

Utilización de NFS

Si se utiliza NFS para establecer comunicación entre la Network Station y el TSF, cuando una Network Station efectúe una petición de un archivo, el TSF empezará a servir este archivo si está en la antememoria. De forma simultánea, verificará que el archivo es de la misma versión que el existente en el servidor de archivos maestro. Si no lo es, el TSF dejará de servir el archivo y empezará inmediatamente a bajar la nueva versión del servidor de archivos maestro.

Si TSF no tiene el archivo en la antememoria, devolverá un mensaje "file not found" (archivo no encontrado). Además, si el archivo solicitado reside en un directorio para el que se ha configurado el TSF con *include subdirectories*, o reside en un subdirectorio bajo un directorio configurado, el TSF empezará a guardar el archivo en antememoria, si el archivo existe en el servidor de archivos maestro.

Actualizaciones de la antememoria de archivos

El protocolo utilizado para la colocación de archivos en antememoria en el IBM 2216 está determinado por la configuración de TSF. Designe un servidor maestro mediante el mandato **add master-file-server**.

Si especifica *rfs*, se le solicitará que proporcione un nombre de archivo de lista de precarga. La lista de precarga es un archivo ASCII que especifica los nombres de archivo calificados al completo de todos los archivos que el TSF debe colocar en la antememoria.

Si especifica *nfs*, se le solicitará que coloque en la antememoria los nombres de directorio (se pueden proporcionar algunos valores por omisión). Cuando especifique un directorio, se le preguntará si desea incluir subdirectorios. Especificar *no* (no incluir subdirectorios) hará que el TSF precargue en la antememoria de TSF todos los archivos que hay en el directorio especificado. Especificar *yes* (incluir subdirectorios) hará que el TSF NO precargue ningún archivo de este directorio, sino que recuperará dinámicamente los archivos de este directorio y cualquiera de sus subdirectorios a medida que las Network Stations soliciten estos archivos.

Los archivos que estén en proceso de renovación, no se enviarán a la Network Station durante este proceso.

Configuración del entorno Thin Server

Cuando se instale el TSF, hay varias configuraciones más allá de la del propio TSF que puede ser necesario tener en cuenta. Esta sección analiza los cambios que pueden ser necesarios para el servidor BootP/DHCP, el servidor de archivos maestro, el IBM 2216 BootP Relay, la dirección IP interna de IBM 2216 y la configuración del TSF IBM 2216. En la sección "Configuración de ejemplo" en la página 584 se analiza un ejemplo de Thin Server que conecta con un AS/400 que ejecuta el Network Station Manager Release 2.5.

Las siguientes secciones describen el proceso de configuración del entorno Thin Server:

- "Recomendaciones sobre la configuración" en la página 582
- "Configuración del servidor BootP/DHCP" en la página 583

- “Configuración del servidor para el entorno Thin Server” en la página 583
- “Configuración de BootP Relay” en la página 583
- “Configuración de la dirección IP interna” en la página 584
- “Configuración del TSF” en la página 584
- “Configuración de ejemplo” en la página 584

Recomendaciones sobre la configuración

A continuación se indican las recomendaciones sobre configuración que le ayudarán a obtener lo máximo del TSF:

- Utilice un disco fijo.

Aunque el TSF no requiere un disco fijo, mejorará el rendimiento si se configura un tamaño demasiado pequeño para la antememoria de la memoria del TSF (o no puede configurarse un tamaño lo bastante grande, a causa de otras funciones en el 2216), y un disco fijo mejorará el rendimiento si el TSF o el 2216 se vuelve a iniciar o a cargar.

- Número máximo de Network Stations.

El TSF permitirá un máximo de 200 conexiones de RFS Network Station a la vez. Encender simultáneamente más de 80 Network Stations puede causar retardos que excedan los valores de tiempo de espera de la Network Station. La recuperación puede requerir que se vuelva a encender la Network Station.

- El servidor de archivos maestro debe ser un servidor que ejecute Network Station Manager.

Aunque el TSF permite que la dirección IP del servidor de archivos maestro tenga cualquier valor, se recomienda que sea la dirección de un dispositivo que ejecute Network Station Manager (NSM), para que la estructura de archivos sea compatible con la Network Station y, por consiguiente, con el TSF y pueda proporcionar los archivos que solicite el TSF.

- Defina memoria suficiente para contener en la memoria todos los archivos colocados en la antememoria.

Esto es obligatorio si no tiene un disco fijo. Si lo tiene, el acceso a la memoria es mucho más rápido que el acceso al disco fijo. La cantidad de memoria necesaria varía según el entorno específico del usuario. Utilice el mandato `Talk 5 list config` para determinar el tamaño del conjunto de archivos en una instancia determinada. El valor visualizado para *Hard File storage being used for Thin Server* es el tamaño del archivo, definido en kilobytes. No obstante, si se añaden o se eliminan del entorno tipos distintos de Network Stations o aplicaciones, este valor puede cambiar.

- Si utiliza NFS, el TSF averigua cuáles son los archivos que necesita.

Este proceso de aprendizaje puede tomar varias secuencias de encendido de la Network Station para que TSF identifique todos los archivos necesarios.

Configuración del servidor BootP/DHCP

Al ejecutar Network Station Manager Release 3, se requiere DHCP cuando se utiliza un Thin Server. Si utiliza un AS/400 como servidor de archivos maestro, puede utilizarse Network Station Manager Release 2.5, en cuyo caso puede utilizarse BootP en lugar de DHCP.

Para BootP, sólo puede especificarse una dirección de servidor. Esta dirección se especifica mediante el código **sa**. Este código puede existir o no en el registro de BootP para una Network Station determinada. Si no existe, créelo y defina el valor como la dirección IP interna del 2216. Si ya existe, cámbielo por la dirección IP interna del 2216.

Para DHCP, los campos que tal vez tengan que modificarse cuando se utilice el Thin Server son los siguientes:

- Opción 66 o servidor de rutina de carga - dirección IP de servidor de código base
Este valor se debe definir como la dirección IP interna del IBM 2216.
- Opción 211 - protocolo para utilizar el servidor de código base
Si se configura el Thin Server para el tipo NFS de servidor de archivos maestro, debe ser *nfs* o *tftp*. Si se está configurando el Thin Server para el tipo RFS del servidor de archivos maestro, debe ser *rfs/400* o *tftp*.
- Opción 212 - servidor de configuración de terminal
Esta dirección debe ser la misma que la dirección IP del servidor de archivos maestro. Esta dirección NO DEBE ser la dirección IP del Thin Server.

Para obtener más detalles acerca de cómo las NS interactúan con BootP y DHCP, consulte el manual *IBM Network Station Manager Installation and Use*, SC41-0664.

Configuración del servidor para el entorno Thin Server

Para RFS, es preciso instalar la lista de precarga en el AS/400. La lista de precarga está disponible en la siguiente dirección de Internet:

<http://www.networking.ibm.com/netprod.html#routers>. Debe ejecutar ftp para el archivo LoadList.file desde este sitio y colocarlo en /QIBM/ProdData/0S400/NetStationRmtController en el AS/400. Es posible que sea necesario crear el directorio NetStationRmtController.

Para NFS, ningún cambio especial es necesario para Thin Server.

Configuración de BootP Relay

Debe habilitarse el agente BootP Relay de IBM 2216 y deben configurarse los servidores BootP y DHCP, de manera que BootP Relay reenviará a estos servidores. Consulte *Nways Multiprotocol Access Services Guía del usuario de software* para obtener más información.

Configuración de la dirección IP interna

Si ya existe una dirección IP interna, no es necesario ningún cambio especial. Si no se especifica ninguna dirección IP interna, debe especificarse una. Consulte *Consulta de configuración y supervisión de protocolos Volumen 1* para obtener más información.

Configuración del TSF

Utilice los mandatos analizados en “Configuración y supervisión de la función Thin Server” en la página 591 para configurar el Thin Server.

Como mínimo, deben entrarse los siguientes mandatos:

1. **load add package thin-server**
2. **set mode enable**
3. **add master-server**

Configuración de ejemplo

El siguiente ejemplo configura un TSF que va a un AS/400 que ejecuta Network Station Manager R2.5.

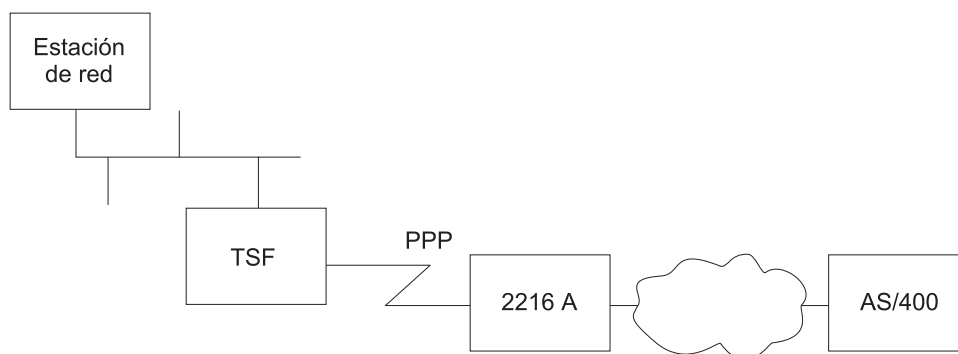


Figura 48. Configuración de ejemplo de TSF

Esta sección describe la configuración de la característica Thin Server, basada en la red antedicha y con las siguientes suposiciones:

- El AS/400 será el servidor BootP.
- El 2216 A es un direccionador (ningún TSF configurado y ninguna configuración especial para TSF).
- Se ha validado la conectividad IP de red, es decir, el AS/400 puede realizar PING en el IBM 2216 (TSF) y el IBM 2216 puede realizar PING en el AS/400.
- BootP Relay NO está habilitado actualmente en el IBM 2216 (TSF)
- Una dirección interna IP NO está configurada actualmente en el IBM 2216 (TSF)

Configuración del AS/400

BootP (NSM Release 2.5)

1. Utilice NSM para definir la NS
2. Ejecute ftp para la tabla BootP a un sistema que tenga un editor ASCII

```
c:\>ftp as400a
Connected to as400a.raleigh.ibm.com.
220-QTCP at AS400A.RALEIGH.IBM.COM.
220 Connection will close if idle more than 5 minutes.
Name (as400a:goofy): qsecofr
331 Enter password. Password:
230 QSECOFR logged on.
ftp> ascii
ftp> get qusrsys/qatodbtp.bootptab bootp.tab
ftp> quit
```

3. Edite el archivo que utiliza un editor ASCII, añadiendo un código "sa" con la dirección IP interna del 2212 (TSF) especificada:

```
OLD LINE
-----
NSEN106:ip=192.9.250.36:bt=IBMNSM:ht=1:ha=00.00.A7.01.2E.35:
sm=255.255.248.0:gw=192.9.250.6:bf=KERNEL:
hd=/QIBM/PRODDATA/NETWORKSTATION

MODIFIED LINE
-----
NSEN106:ip=192.9.250.36:bt=IBMNSM:ht=1:ha=00.00.A7.01.2E.35:
sm=255.255.248.0:gw=192.9.250.6:bf=KERNEL:
hd=/QIBM/PRODDATA/NETWORKSTATION:sa=192.9.250.6
```

donde 192.9.250.6 es la dirección IP interna del 2212 (TSF)

4. Ejecute ftp para devolver la tabla BootP al AS/400

```
c:\> ftp as400a
Connected to as400a.raleigh.ibm.com.
220-QTCP at AS400A.RALEIGH.IBM.COM.
220 Connection will close if idle more than 5 minutes.
Name (as400a:goofy): qsecofr
331 Enter password.
Password:
230 QSECOFR logged on.
ftp> ascii
ftp> put bootp.tab qusrsys/qatodbtp.bootptab
ftp> quit
```

Configuración de la lista de precarga

Puede obtener una lista de precarga de Internet en:
<http://www.networking.ibm.com/netprod.html#routers>

Una vez que tenga la lista de precarga, puede ejecutar "ftp" para enviarla al AS/400.

1. Asegúrese de que el directorio local esté definido en la ubicación del archivo "LoadList.file".
2. Ejecute ftp al AS/400 - "test400" es el nombre del AS/400 en este ejemplo.

```
ftp test400
Connected to test400.raleigh.ibm.com.
Name (test400:root): qsecofr
Enter password.
Password:
QSECOFR logged on.
```

3. Cambie al directorio correcto en el AS/400 de destino:

```
ftp> cd /
Current directory changed to /.
ftp> cd qibm/proddata/os400/
Current directory changed to /qibm/proddata/os400.
ftp> dir
PORT subcommand request successful.
List started.
QTCP          34816 04/30/97 02:50:36 *DIR    REXEC/
QSECOFR       33792 07/24/98 08:04:55 *DIR    NetStationRmtController/
List completed.
```

4. Si el directorio "NetStationRmtController" no existe, tendrá que crearlo.

```
ftp> MKD
(directory - name) NetStationRmtController
Created directory /qibm/proddata/os400/netstationrmtcontroller
```

5. Cambie al directorio NetStationRmtController:

```
ftp> cd NetStationRmtController
Current directory changed to /qibm/proddata/os400/Netstationrmtcontroller.
```

6. Transfiera el archivo al AS/400:

```
ftp> ascii
Representation type is ASCII nonprint.
ftp> put LoadList.file
PORT subcommand request successful.
Sending file to /qibm/proddata/os400/Netstationrmtcontroller
File transfer completed successfully.
```

Configuración de TCP/IP

La configuración de TCP/IP dependerá de su entorno específico.

Configuración del IBM 2216 (TSF)

BootP Relay

1. Determine si BootP Relay ya está configurado:

```
*
*
t 6
Config>protocol ip Internet protocol user configuration
IP config>list bootp
BOOTP forwarding: enabled
Max number of BOOTP forwarding hops: 4
Min secs of retry before forwarding: 0
Configured BOOTP servers:      192.9.220.21
IP config>
```

2. Si no está habilitado ya, habilítelo:

```
IP config>enable bootp
Maximum number of forwarding hops [4]?
Minimum seconds before forwarding [0]?
IP config>
```

3. Si el servidor BootP o DHCP de Network Station no está en la lista de los servidores configurados, añádalo:

```
IP config>add bootp-server
BOOTP server address [0.0.0.0]? 9.37.121.6
IP config>
```

Dirección IP interna

1. Determine si ya se ha configurado una dirección IP interna:

```
Config>protocol ip
Internet protocol user configuration
IP config>list addresses
IP addresses for each interface:
  intf    0   9.37.177.97   255.255.248.0   Local wire...
  intf    1  192.9.220.2    255.255.255.0   Local wire...
  intf    2  192.9.250.6    255.255.255.0   Local wire...
  intf    3  192.9.222.2    255.255.255.0   Local wire...
  intf    4                               IP disabled...
  intf    5                               IP disabled...
  intf    6  192.9.223.2    255.255.255.0   Local wire...
IP config>
```

2. Configure la dirección IP interna.

```
IP config>set internal-ip-address
Internal IP address [192.9.223.2]? 192.9.250.6
IP config>
```

3. Liste de nuevo las direcciones.

```
IP config>list addresses
IP addresses for each interface:
  intf    0   9.37.177.97   255.255.248.0   Local wire
  intf    1  192.9.220.2    255.255.255.0   Local wire
  intf    2  192.9.250.6    255.255.255.0   Local wire
  intf    3  192.9.222.2    255.255.255.0   Local wire
  intf    4                               IP disabled
  intf    5                               IP disabled
  intf    6  192.9.223.2    255.255.255.0   Local wire
Internal IP address: 192.9.250.6
IP config>
```

Característica Thin Server

1. Add load package thin-server

Antes de que pueda configurarse la característica Thin Server, debe añadir el paquete de carga.

En primer lugar, asegúrese de que el paquete de Thin Server está disponible.

```
Config>load list available Available Packages
-----
appn package
tn3270e package
thin-server package
Config>
```

Si no está disponible, tendrá que obtener la versión correcta del software antes de continuar.

Si está disponible, verifique que el paquete no está cargado.

```
Config>load list configured
Configured Packages
-----
thin-server package
Config>
```

Si ya está cargado/configurado (como se muestra anteriormente), puede continuar configurando el TSF. Si no se ha cargado ya, tendrá que añadir el paquete de Thin Server:

```
Config>load add package thin-server
thin-server package configured successfully
This change requires a reload.
Config>
```

2. Reload

Si tuvo que añadir el paquete de Thin Server, debe escribir la configuración y volver a cargar el IBM 2216.

3. Set mode enable

Cuando se cargue el paquete, inicialmente el Thin Server está inhabilitado. La modalidad se debe definir como habilitada antes de que pueda configurarse cualquier otro parámetro de Thin Server.

```
*
*
t 6
Config>feature tsf
Thin server config>set mode enable

Thin server feature (TSF) is fully enabled once
you have entered a Master File Server for either
RFS or NFS. Please add a master-file-server if
one is not already configured.
Thin server config>
```

4. Add master-file-server.

Una vez que esté habilitada la característica Thin Server, es preciso configurar el servidor de archivos maestro. En este caso, el servidor de archivos maestro es un AS/400, por lo que añadiremos un servidor de archivos maestro de RFS. Para esta red, los parámetros de tiempo de espera y reintento de TFTP por omisión son adecuados.

```
Thin server config>add master-file-server rfs-as400
File Server IP address [0.0.0.0]? 9.37.100.68
TFTP Packet Timeout in seconds (5 - 10) [5]?
TFTP Max Retry Limit (1 - 10) [1]? 7
TFTP Max Segment Size in bytes (valid values are 512, 1024, 2048, 4096, 8192)
[8192]?
Pre-load File name
[/QIBM/ProdData/OS400/NetstationRmtController/Load list.file]?
Thin server config>
```

La dirección IP de nuestro AS/400 en la interfaz de Red en Anillo es 9.37.100.68. Cuando instalamos el archivo de lista de precarga en el AS/400, asignamos su nombre de manera que coincidiese con el nombre por omisión del Thin Server, de manera que no sea necesario modificarlo.

5. Set time-to-refresh-pre-load-list (opcional)

El valor por omisión de la hora del día para realizar la renovación es la 1:00 AM. Esto se ha elegido así para minimizar los impactos de rendimiento, si se han modificado archivos grandes y es preciso que el Thin Server tenga que bajarlo.

6. Set interval-pre-load-list (opcional)

El intervalo por omisión para verificar que los archivos en antememoria estén al mismo nivel que el servidor de archivos maestro es diario. El valor de este parámetro y el del parámetro time-to-refresh-pre-load-list determinan con qué frecuencia se verifican los archivos. Si los archivos de la Network Station cambian en raras ocasiones, tal vez desee definirlos para renovarlos sólo una vez a la semana o al mes.

7. Set memory (opcional).

La memoria por omisión de una antememoria de RAM de 16 MB para la antememoria de archivos debería ser suficiente. Cuando varias Network

Stations utilicen el TSF, consulte “Recomendaciones sobre la configuración” en la página 582 para conocer los valores recomendados.

8. Set hard file (opcional)

Se recomienda un disco fijo. Si no tiene un disco fijo, este parámetro se debe definir como *no*.

Configuración y supervisión de la función Thin Server

Este capítulo describe cómo utilizar los mandatos operativos y de configuración de la función Thin Server (TSF) y contiene las secciones siguientes:

- “Acceso al entorno de configuración de TSF”
- “Mandatos de configuración de TSF”
- “Acceso al entorno de supervisión de TSF” en la página 601
- “Mandatos de supervisión de TSF” en la página 601

Acceso al entorno de configuración de TSF

Utilice el siguiente procedimiento para acceder al proceso de configuración del TSF.

1. En el indicador OPCON, entre **talk 6**. (Para obtener más detalles sobre este mandato, consulte “The OPCON Process and Commands” en el manual *Nways Multiprotocol Access Services Guía del usuario de software*.) Por ejemplo:

```
* talk 6
Config>
```

Después de entrar el mandato **talk 6**, el indicador CONFIG (Config>) se visualiza en la terminal. Si el indicador no aparece al entrar la configuración por primera vez, pulse de nuevo **Return**.

2. En el indicador CONFIG, entre el mandato **feature tsf** para acceder al indicador Thin server config>.

Mandatos de configuración de TSF

Para configurar TSF, entre los mandatos en el indicador Thin server config>.

Tabla 64. Resumen de los mandatos de configuración del TSF

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxiv.
Add	Añade el servidor de archivos maestro (RFS o NFS).
Delete	Suprime el servidor de archivos maestro (RFS o NFS).
List	Lista la configuración del Thin Server.
Modify	Modifica el servidor de archivos maestro (RFS o NFS).
Set	Define los parámetros del Thin Server.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiv.

Add

Utilice el mandato **add** para añadir una configuración del servidor de archivos maestro.

Si selecciona *nfs* como tipo de servidor de archivos maestro, el Thin Server utilizará NFS para establecer comunicación con el servidor de archivos maestro y los archivos de sincronización y las NS podrán establecer comunicación con el Thin Server utilizando TFTP o NFS. Si selecciona *rfs* como tipo de servidor de archivos maestro, el Thin Server utilizará RFS para establecer comunicación con el servidor de archivos maestro y los archivos de sincronización y las NS podrán establecer comunicación con el Thin Server utilizando TFTP o RFS.

Sintaxis:

```
add master-file-server nfs-s390  
                          nfs-nt  
                          nfs-aix  
                          nfs-other  
                          rfs-as400
```

nfs-s390 Se utiliza cuando el TSF está conectado a un S/390.

file server IP address

Valores válidos: cualquier dirección IP válida

Valor por omisión: ninguno

tftp packet timeout

Valores válidos: 5 - 10 segundos

Valor por omisión: 5

tftp maximum retry limit

Valores válidos: 1 - 10

Valor por omisión: 1

maximum segment size

Especifica el tamaño máximo de segmento de paquete.

Valores válidos: 512, 1024, 2048, 4096, 8192 (bytes)

Valor por omisión: 8192

additional Include subdirectories

Especifica si se han de añadir subdirectorios incluidos adicionales. Se pueden especificar los subdirectorios adicionales si el TSF tiene que colocar archivos en antememoria que no están en los directorios por omisión.

Valores válidos: yes o no

Valor por omisión: yes

additional Include subdirectory path

Especifica la vía de acceso del subdirectorio de inclusión que se va a añadir.

Valores válidos: a-z, A-Z, 0-9, ., _, —, /

Valor por omisión: ninguno

include all subdirectories under this directory

Especifica si se incluirán todos los subdirectorios anidados en la vía de acceso de subdirectorio adicional especificado.

Valores válidos:

- No
El TSF precargará todos los archivos en el directorio especificado.
- Yes
El TSF no precargará ningún archivo en el directorio especificado. En cambio, el TSF cargará archivos desde el directorio y cualquiera de sus subdirectorios, según sea necesario.

Valor por omisión: no

nfs-nt Se utiliza cuando el TSF está conectado a Windows-NT.

file server IP address

Valores válidos: cualquier dirección IP válida

Valor por omisión: ninguno

tftp packet timeout

Valores válidos: 5 - 10 segundos

Valor por omisión: 5

tftp maximum retry limit

Valores válidos: 1 - 10

Valor por omisión: 1

maximum segment size

Especifica el tamaño máximo de segmento de paquete.

Valores válidos: 512, 1024, 2048, 4096, 8192 (bytes)

Valor por omisión: 8192

additional Include subdirectories

Especifica si se han de añadir subdirectorios incluidos adicionales.

Valores válidos: yes o no

Valor por omisión: yes

additional Include subdirectory path

Especifica la vía de acceso del subdirectorio de inclusión que se va a añadir.

Valores válidos: a-z, A-Z, 0-9, ., _, —, /

Valor por omisión: ninguno

include all subdirectories under this directory

Especifica si se incluirán todos los subdirectorios anidados en la vía de acceso de subdirectorio adicional especificado.

Valores válidos:

- No
El TSF precargará todos los archivos en el directorio especificado.
- Yes
El TSF no precargará ningún archivo en el directorio especificado. En cambio, el TSF cargará archivos desde el directorio y cualquiera de sus subdirectorios, según sea necesario.

Valor por omisión: no

nfs-aix Se utiliza cuando el TSF está conectado a AIX.

file server IP address

Valores válidos: cualquier dirección IP válida

Valor por omisión: ninguno

tftp packet timeout

Valores válidos: 5 - 10 segundos

Valor por omisión: 5

tftp maximum retry limit

Valores válidos: 1 - 10

Valor por omisión: 1

maximum segment size

Especifica el tamaño máximo de segmento de paquete.

Valores válidos: 512, 1024, 2048, 4096, 8192 (bytes)

Valor por omisión: 8192

additional Include subdirectories

Especifica si se han de añadir subdirectorios incluidos adicionales.

Valores válidos: yes o no

Valor por omisión: yes

additional Include subdirectory path

Especifica la vía de acceso del subdirectorio de inclusión que se va a añadir.

Valores válidos: a-z, A-Z, 0-9, ., _, —, /

Valor por omisión: ninguno

include all subdirectories under this directory

Especifica si se incluirán todos los subdirectorios anidados en la vía de acceso de subdirectorio adicional especificado.

Valores válidos:

- No
El TSF precargará todos los archivos en el directorio especificado.
- Yes
El TSF no precargará ningún archivo en el directorio especificado. En cambio, el TSF cargará archivos desde el directorio y cualquiera de sus subdirectorios, según sea necesario.

Valor por omisión: no

nfs-other Se utiliza cuando se desea designar manualmente todos los subdirectorios.

file server IP address

Valores válidos: cualquier dirección IP válida

Valor por omisión: ninguno

tftp packet timeout

Valores válidos: 5 - 10 segundos

Valor por omisión: 5

tftp maximum retry limit

Valores válidos: 1 - 10

Valor por omisión: 1

maximum segment size

Especifica el tamaño máximo de segmento de paquete.

Valores válidos: 512, 1024, 2048, 4096, 8192 (bytes)

Valor por omisión: 8192

additional Include subdirectories

Especifica si se han de añadir subdirectorios incluidos adicionales.

Valores válidos: yes o no

Valor por omisión: yes

additional Include subdirectory path

Especifica la vía de acceso del subdirectorio de inclusión que se va a añadir.

Valores válidos: a-z, A-Z, 0-9, ., _, —, /

Valor por omisión: ninguno

include all subdirectories under this directory

Especifica si se incluirán todos los subdirectorios anidados en la vía de acceso de subdirectorio adicional especificado.

Valores válidos:

- No

El TSF precargará todos los archivos en el directorio especificado.

- Yes

El TSF no precargará ningún archivo en el directorio especificado. En cambio, el TSF cargará archivos desde el directorio y cualquiera de sus subdirectorios, según sea necesario.

Valor por omisión: no

rfs-as400 Se utiliza cuando el TSF está conectado a un AS/400.

file server IP address

Valores válidos: cualquier dirección IP válida

Valor por omisión: ninguno

tftp packet timeout

Valores válidos: 5 - 10 segundos

Valor por omisión: 5

tftp maximum retry limit

Valores válidos: 1 - 10

Valor por omisión: 1

maximum segment size

Especifica el tamaño máximo de segmento de paquete.

Valores válidos: 512, 1024, 2048, 4096, 8192 (bytes)

Valor por omisión: 8192

pre-load file name

Especifica el nombre y la vía de acceso del archivo de pre-carga.

Valores válidos: a-z, A-Z, 0-9, ., _, —, / **Valor por omisión:** /QIBM/ProdData/OS400/NetStationRmtController/LoadList.file

Ejemplo: para NFS

```
Thin server config> add master-file-server nfs
File Server IP address [0.0.0.0]? 10.22.55.94
TFTP Packet Timeout in seconds (5 - 10) [5]? 6
TFTP Max Retry Limit (1 - 10) [1]? 7
TFTP Max Segment Size in bytes (valid values are 512, 1024, 2048, 4096, 8192) [8192]? 512
```

Default Include Directories:

Include Directory List Follows:

```
Include
all
Subdirs?  Directory Names
-----  -----
N        /hfs/usr/lpp/nstation/standard
Y        /hfs/usr/lpp/nstation/standard/mods
Y        /hfs/usr/lpp/nstation/standard/nls
Y        /hfs/usr/lpp/nstation/standard/fonts
Y        /hfs/usr/lpp/nstation/standard/java
Y        /hfs/usr/lpp/nstation/standard/keyboards
Y        /hfs/usr/lpp/nstation/standard/proms
Y        /hfs/usr/lpp/nstation/standard/X11
Y        /hfs/usr/lpp/nstation/standard/configs
Y        /hfs/usr/lpp/nstation/standard/SysDef
Y        /hfs/usr/lpp/nstation/standard/zoneinfo
Do you want additional Include Subdirectories (Y)es (N)o? [y]
```

```
Include Subdirectory [ ]? /usr/lpp/nstation/standard/whatever
Include all subdirectories under this directory (Y)es or (N)o? [n]
```

Do you want additional Include Subdirectories (Y)es (N)o? []

Ejemplo: para RFS

```
Thin server config> add master-file-server rfs
File Server IP address [0.0.0.0]? 01.01.01.98
TFTP Packet Timeout in seconds (5-10) [5]? 6
TFTP Max Retry Limit (1-10) [1]? 7
TFTP Max Segment Size in bytes (valid values are 512, 1024, 2048, 4096, 8192) [8192]? 512

Pre-Load File name
[/QIBM/ProdData/OS400/NetStationRmtController/LoadList.file]?
```

Delete

Utilice el mandato **delete** para eliminar una configuración del servidor de archivos maestro.

Sintaxis:

```
delete master-file-server nfs
                        rfs
```

nfs Se utiliza cuando se configura cualquiera de los servidores de archivos maestros de NFS.

rfs Se utiliza cuando se configura el TSF para el servidor de archivos maestro de RFS.

Mandatos de configuración de TSF (Talk 6)

List

Utilice el mandato **list** para visualizar la configuración de TSF.

Sintaxis:

list all

Ejemplo:

```
Thin server config> list all
```

Thin Server Feature:

```
Enabled
Interval to refresh cache in day(s): 2
Time of day (military time) to refresh cache: 0800
Megabytes used for Thin Server RAM cache: 4
Use Hard File: YES
```

Master Thin Server list:

```
Server IP Address: 9.37.111.12
Server Protocol: NFS
TFTP Packet Timeout in seconds: 10
TFTP Retry Limit           : 6
TFTP Max Segment Size in bytes: 512
```

Initial directories setup for server type: NFS-AIX

NFS Include Directory List Follows:

```
Include
  all
subdirs?  Directory Names
-----  -
```

N	/usr/netstation
Y	/usr/netstation/mods
Y	/usr/netstation/nls
Y	/usr/netstation/fonts
Y	/usr/netstation/java
Y	/usr/netstation/keyboards
Y	/usr/netstation/proms
Y	/usr/netstation/X11
Y	/usr/netstation/configs
Y	/usr/netstation/SysDef
Y	/usr/netstation/zoneinfo

Modify

Utilice el mandato **modify** para modificar una configuración del servidor de archivos maestro.

Sintaxis:

```
modify master-file-server nfs
                               rfs
```

nfs Se utiliza cuando se ha configurado uno de los servidores de archivos maestros de NFS.

rfs Se utiliza cuando se configura el TSF para el servidor de archivos maestro de RFS.

Ejemplo: para NFS

```
Thin server config> modify master-file-server nfs
File Server IP address [          ]? 10.22.55.94
TFTP Packet Timeout in seconds (5 - 10) [5 ]? 10
TFTP Max Retry Limit (1 - 10) [1]? 6
TFTP Max Segment Size in bytes valid values are 512, 1024, 2048, 4096,
8192) [8192]? 1024

Include subdirectory [/usr/lpp/tcpip/nstation/standard, (Y)es or (N)o [Y]?
    Include all subdirectories under this directory (Y)es or (N)o [N]?

Include subdirectory [/usr/lpp/tcpip/nstation/standard/mods], (Y)es or (N)o [Y]?
    Include all subdirectories under this directory (Y)es or (N)o [N]?

Include subdirectory [/usr/lpp/tcpip/nstation/standard/nls], (Y)es or (N)o [Y]?
    Include all subdirectories under this directory (Y)es or (N)o [N]?

Include subdirectory [/usr/lpp/tcpip/nstation/standard/fonts], (Y)es or (N)o [Y]?
    Include all subdirectories under this directory (Y)es or (N)o [N]?

Include subdirectory [/usr/lpp/tcpip/nstation/standard/java], (Y)es or (N)o [Y]?
    Include all subdirectories under this directory (Y)es or (N)o [N]?

Include subdirectory [/usr/lpp/tcpip/nstation/standard/keyboards], (Y)es or (N)o [Y]?
    Include all subdirectories under this directory (Y)es or (N)o [N]?

Do you want additional Include Subdirectories (Y)es or (N)o? n
```

Ejemplo: para RFS

```
Thin server config> modify master-file-server rfs
File Server IP address [09.09.255.253 ]? 01.01.01.98
TFTP Packet Timeout in seconds [5 ]? 10
TFTP Retry Limit [5 ]? 6
TFTP Max Segment Size in bytes [8192]? 512

Pre-Load File name
[/QIBM/ProdData/OS400/NetStationRmtController/LoadList.file]?

```

Set

Utilice el mandato **set** para definir los parámetros de configuración de TSF.

Sintaxis:

```
set          mode
              interval-pre-load-list
              time-to-refresh-pre-load-list
              memory-cache
              hard-file
```

mode Especifica la modalidad del TSF.

Valores válidos:

- enable

La modalidad enable (habilitar) quiere decir que el TSF es totalmente funcional y servirá los archivos de antememoria a las Network Stations.

- disable

Mandatos de configuración de TSF (Talk 6)

La modalidad disable (inhabilitar) quiere decir que el TSF no está activo y no responderá a ninguna Network Station. Las Network Stations se deben configurar para establecer comunicación directa con el servidor.

- **passthru**

La modalidad passthru (paso a través) sólo es válida al utilizar RFS. El paso a través permitirá que la Network Station pueda establecer contacto con el TSF, pero siempre obtendrá archivos del servidor de archivos maestro.

Valor por omisión:

interval-pre-load-list

Especifica el intervalo para renovar la lista de precarga, medido en días.

Valores válidos: 00 - 365

Valor por omisión: 01

time-to-refresh-pre-load-list

Especifica la hora del día en formato de 24 horas para renovar la antememoria.

Valores válidos: 0001 - 2400

Valor por omisión: 0100

memory-cache

Especifica la cantidad de memoria en megabytes para la antememoria de RAM del Thin Server. Al utilizar un disco fijo, se debe elegir este valor para equilibrar el rendimiento del TSF con otras funciones del IBM 2216. Cuando no se utiliza un disco fijo, este valor debe ser lo bastante grande para contener todos los archivos en la antememoria. Para obtener más información, consulte "Recomendaciones sobre la configuración" en la página 582.

Valores válidos: 8 - 64 Megabytes

Valor por omisión: 16

hard-file Especifica si se debe utilizar el disco fijo.

Valores válidos: yes o no

Valor por omisión: yes

Ejemplo:

```
Thin server config> set mode passthru
This server feature (TSF) is passthru
Thin server config> set interval-pre-load-list
Interval to refresh the Pre-Load list in days (00-365) [01]? 1
Thin server config> set time-to-refresh-pre-load-list
Time of day to refresh cache in military time (0001-2400) [0100] 0800
Thin server config> set memory-cache
Amount of memory in megabytes for Thin Server RAM cache (8-64MB) [8]
Thin server config> set hard-file
Use the Hard File (Y)ex N(o) [Y]? yes
```

Acceso al entorno de supervisión de TSF

Utilice el siguiente procedimiento para acceder a los mandatos de supervisión de TSF. Este proceso proporciona acceso al proceso de *supervisión* del TSF.

1. En el indicador OPCON, entre **talk 5**. (Para obtener más detalles sobre este mandato, consulte *The OPCON Process and Commands* en el manual Nways Multiprotocol Access Services Guía del usuario de software.) Por ejemplo:

```
* talk 5
+
```

Después de entrar el mandato **talk 5**, el indicador GWCON (+) se visualiza en la terminal. Si el indicador no aparece al entrar la configuración por primera vez, pulse de nuevo **Return**.

2. En el indicador +, entre el mandato **f tsf** para acceder al indicador Thin-Server>.

Ejemplo:

```
+ f tsf
Thin-Server>
```

Mandatos de supervisión de TSF

Esta sección describe los mandatos de supervisión de TSF.

Tabla 65. Resumen de los mandatos de supervisión del TSF

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado "Cómo obtener ayuda" en la página xxxiv.
Delete	Suprime un archivo de la antememoria de archivos de la característica Thin Server.
Flush	Desecha el contenido de la antememoria de archivos de la característica Thin Server.
List	Visualiza los valores de Thin Server.
Refresh	Renueva la antememoria.
Reset	Restablece los contadores.
Restart	Reinicia el proceso de Thin Server.
Set	Cambia los valores de la característica Thin Server.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado "Cómo salir de un entorno de nivel inferior" en la página xxxiv.

Delete

Utilice el mandato **delete** para eliminar un archivo de la antememoria de archivos de la característica Thin Server.

Sintaxis:

```
delete                    nombre-archivo
```

Mandatos de supervisión de TSF (Talk 5)

nombre-archivo

Especifica el nombre del archivo que se debe eliminar de la antememoria de archivos.

Valores válidos:

Valor por omisión: ninguno

Ejemplo:

```
Thin-Server> delete
Enter filename to delete from the File Cache: /ibm/prod/ns/5494.dat
Are you sure that you want to delete this file? (Y/ [N]): y
File successfully deleted
```

Flush

Utilice el mandato **flush** para desechar la memoria del TSF y el espacio de antememoria del disco duro. El mandato **flush** borrará todos los archivos de antememoria. La antememoria de Thin Server se actualizará en la siguiente renovación del Servidor maestro. Las Network Stations pueden sufrir retardos hasta que se complete la renovación.

Sintaxis:

flush

Ejemplo:

```
Thin-Server> flush
The FLUSH command will erase all cached files.
The Thin Server cache will be updated on the next refresh
from the Master Server. Network Stations may experience
delays until the refresh is completed.
Are you sure you really want to do this? (Y/ [N]): y
All Thin Server cached files have been flushed
```

List

Utilice el mandato **list** para visualizar los valores de parámetros de TSF.

Sintaxis:

list cached-files
 config
 file-access-counters
 file-refresh-counters
 pre-load-list
 tftp-counters
 ts-counters

Ejemplo:

```
Thin-Server> list cached-files
```

```

Cached
File Name      File Size  Time Stamp      Flags  Host File Name
-----
00000026.DAT   2729      04/08/98 13:35:07   RYY   /QIBM/ProdData/OS400/Netstat
ionRmtController/Loadlist.file
00000002.DAT   2049220   09/16/97 08:55:39   RYU   /QIBM/PRODDATA/NETWORKSTATIO
N/KERNEL
              10060   03/04/97 16:12:44   RY-   /QIBM/PRODDATA/NETWORKSTATIO
N/FONTS/PCF/MISC/7X14B.PCF
List is Complete

```

Los distintivos tienen el siguiente significado:

- WhereFrom
 - R = Cliente RFS
 - N = Cliente NFS
 - - = Ninguno
- InTable
 - - = No está en la tabla
 - u (o m) = A punto de actualizarse
 - Y = En la tabla
- FileState
 - - = No en el disco
 - D = Sucio
 - A = Actualización cancelada
 - u = A punto de actualizarse
 - U = Actualización en proceso
 - Y = En el disco y disponible

Las combinaciones comunes de los dos últimos distintivos (los tres distintivos se muestran por razones de claridad) son:

- RYY - archivo en buen estado
- RuY - renovación completa en proceso, este archivo no se ha verificado aún
- RYU - se está actualizando este archivo

Mandatos de supervisión de TSF (Talk 5)

Ejemplo: para RFS

```
Thin-Server> list config
Thin Server Configuration
  Thin Server feature is:                Enabled
  Thin Server feature state is:          Active, initializing file structure
  Interval to refresh Pre-Load List (#days): 1
  Time of day (Military) to refresh Pre-Load List: 01:00:00
  Memory (KB) currently using for RAM cache: 25600
  Maximum memory (KB) configured for RAM cache: 25600
  Currently using Hard File?:           Yes
  Hard File storage defined for Thin Server: 942752
  Hard File storage being used for Thin Server: 0
  Number of Files Cached:                0
  Master Server IP address:              9.37.177.61
  TFTP Packet Timeout Value:             5
  TFTP Max Retries:                      1
  TFTP Max Segment Size:                 8192

  Thin Server Sync Protocol:             RFS
  Name of Pre-Load List file:
    /QIBM/ProdData/OS400/NetstationRmtController/Loadlist.file
Thin Server>
```

Ejemplo: para NFS

```
Thin-Server> list config
Thin Server Configuration
  Thin Server feature is:                Enabled
  Thin Server Feature state is:          Active, initializing file structure
  Interval to refresh Pre-Load List (#days): 1
  Time of day (Military) to refresh Pre-Load List: 01:00:00
  Memory (KB) currently using for RAM cache: 25600
  Maximum memory (KB) configured for RAM cache: 25600
  Currently using Hard File?:           Yes
  Hard File storage defined for Thin Server: 915424
  Hard File storage being used for Thin Server: 27328
  Number of Files Cached:                82
  Master Server IP address:              9.37.181.47
  TFTP Packet Timeout Value:             5
  TFTP Max Retries:                      1
  TFTP Max Segment Size:                 8192

  Thin Server Sync Protocol:             NFS
  Include Directory List Follows:

  Include
  all
  Subdirs?  Directory Names
  -----  -----
  N         /usr/netstation
  Y         /usr/netstation/mods
  Y         /usr/netstation/nls
  Y         /usr/netstation/fonts
  Y         /usr/netstation/java
  Y         /usr/netstation/keyboards
  Y         /usr/netstation/proms
  Y         /usr/netstation/X11
  Y         /usr/netstation/configs
  Y         /usr/netstation/SysDef
  Y         /usr/netstation/zoneinfo
Thin Server>
```


Ejemplo:Thin-Server> **list file-access-counters**

```

Disk Statistics/Counters:
  Number of files currently open:          20
  Number of Total File Opens:            23
  Number of Open Fails when File is Locked: 1
  Number of Read misses - Version Mismatch: 4
  Number of Read misses - File Not Present: 3
  Number of Write misses - Hard File Full: 4

```

Ejemplo:Thin-Server> **list file-refresh-counters**

```

File Refresh Statistics/Counters
  Number of Files Updated during last refresh: 0
  Number of Update Failures during last refresh: 0
  Number of Refreshes: 0
  Number of Refresh Failures: 1
  Number of Files Refreshed: 30
  Date/Time of Last File Update: has not occurred since last reset
  Date/Time of Last File Download: has not occurred since last reset

```

Thin Server>

Ejemplo:

```

Thin-Server> list pre-load-list
<display of pre-load list raw file>
List of Pre-Load List File is Complete

```

Ejemplo:Thin-Server> **list tftp-counters**

```

TFTP Statistics/Counters
  Number of Total TFTP Clients: 3
  Number of Current TFTP Clients: 2
  Number of Files Served: 22
  Number of Files Served by Master Server: 22

```

Ejemplo: para RFSThin-Server> **list ts-counters**

```

Thin Server Statistics/Counters
  Relay to Master File Server: Available
  Number of Total RFS Clients: 0
  Number of Current RFS Clients: 0
  Number of Files Served: 0
  Number of Files Served by Master Server: 0
  Number of NS Port Mapper socket accepts: 0
  Number of NS Port Mapper sockets currently active/open: 0
  Number of NS Server socket accepts: 0
  Number of NS 8473 sockets currently active/open: 0
  Number of NS Login sock accepts: 0
  Number of NS 8476 sockets currently active/open: 0
  Number of RFS writes to a Thin Server cached file: 0

```

Thin Server>

Mandatos de supervisión de TSF (Talk 5)

Ejemplo: para NFS

```
Thin-Server> list ts-counters
```

```
Thin Server Statistics/Counters
Number of NFS Server Reads:          13
Number of NFS Server Read Directories: 8
Number of Unsupported NFS Requests:  2
Number of total NFS Mounts:          22
Number of current NFS Mounts:        7
Number of total NFS clients:         15
Number of current NFS Clients:        4
```

Refresh

Utilice el mandato **refresh** para forzar la renovación de la antememoria.

Sintaxis:

refresh

Ejemplo:

```
Thin-Server> refresh
```

```
Force a refresh of the cache ? (Y/ [N]): y
```

```
Thin Server cache has been refreshed
```

Reset

Utilice el mandato **reset** para restaurar los contadores dinámicamente.

Sintaxis:

```
reset          all
                 file-access-counters
                 file-refresh
                 tftp-counters
                 ts-counters
```

Ejemplo:

```
Thin-Server> reset all
```

```
All Thin Server feature counters have been reset
```

Restart

Utilice el mandato **restart** para reiniciar el proceso de TSF.

Sintaxis:

restart

Ejemplo:

```
Thin-Server> restart
```

```
Restart Thin Server? (Y/ [N]): y
```

```
Thin Server has been restarted
```

Set

Utilice el mandato **set** para definir la modalidad de colocación en antememoria de TSF.

Sintaxis:

set mode

mode Especifica la modalidad del TSF. Vea "Set" en la página 599.

Valores válidos:

- enable
- disable
- passthru

Ejemplo:

```
Thin-Server> set mode ?
```

```
DISABLED  
ENABLED  
PASSTHRU
```

```
Thin-Server> set mode disable
```

```
Thin Server caching is now disabled
```

Mandatos de supervisión de TSF (Talk 5)

Configuración y supervisión de VCRM

El Gestor de recursos de circuito virtual (VCRM) es una característica que da soporte al Resource ReSerVation Protocol (RSVP), que se describe en las secciones "Using RSVP" y "Configuring and Monitoring RSVP" del manual *Consulta de configuración y supervisión de protocolos Volumen 1*. VCRM, basándose en la petición de reserva de RSVP, crea la conexión para el flujo de datos a través de la interfaz física. Para ello, VCRM debe determinar en primer lugar si el ancho de banda es suficiente para acomodar la reserva.

Nota: Si utiliza interfaces de WAN, como Frame Relay o X.25, tiene que definir la velocidad de línea para que VCRM sepa de cuánto ancho de banda dispone. El procedimiento para definir la velocidad de línea está descrito en los capítulos que tratan de la configuración y supervisión de las interfaces Frame Relay y X.25 del manual *Nways Multiprotocol Access Services Guía del usuario de software*.

Si la interfaz es ATM SVC, VCRM correlaciona las peticiones de QoS RSVP con las peticiones de configuración de SVC. La petición de reserva de RSVP es satisfactoria si también lo es la configuración de SVC. VCRM asegura que haya un espacio de almacenamiento intermedio adecuado para los paquetes de QoS, y que estos paquetes se envíen a través del SVC correcto para su transmisión.

Si la interfaz no es ATM, como un enlace PPP, LAN o WAN, VCRM utiliza el sistema de colas de software de QoS y los paquetes de mejor esfuerzo para dar prioridad a los paquetes que se encuentran en el enlace de salida.

Este capítulo incluye las secciones siguientes:

- "Acceso al entorno de configuración de VCRM"
- "Acceso al entorno de supervisión de VCRM"
- "Mandatos de supervisión de VCRM" en la página 610

Acceso al entorno de configuración de VCRM

Para acceder al entorno de configuración de VCRM, entre el mandato siguiente en el indicador Config>:

```
Config> feature vcrm
VC & Resource Management config console
--Currently no configurable objects.
Config>
```

El propósito del mensaje visualizado es indicarle que VCRM no se puede configurar por separado. La habilitación de RSVP habilita también VCRM, el cual obtiene sus parámetros de la configuración de RSVP.

Acceso al entorno de supervisión de VCRM

Para acceder al entorno de supervisión de VCRM, escriba

```
* t 5
```

A continuación, entre el siguiente mandato en el indicador +:

```
+ feature VCRM
VCRM console
VCRM Console>
```

Aparece el indicador VCRM Console>.

Mandatos de supervisión de VCRM

Esta sección describe los mandatos de supervisión de VCRM. Entre estos mandatos en el indicador VCRM Console>.

Tabla 66. Mandatos de supervisión de VCRM

Mandato	Función
? (Help)	Visualiza todos los mandatos disponibles para este nivel de mandatos o lista las opciones para mandatos específicos (si están disponibles). Consulte el apartado “Cómo obtener ayuda” en la página xxxiv.
Clear	Restablece las estadísticas de cola.
Queue	Muestra las estadísticas de las colas de software que no son ATM.
Exit	Le devuelve al nivel de mandatos anterior. Consulte el apartado “Cómo salir de un entorno de nivel inferior” en la página xxxiv.

Clear

Utilice el mandato **clear** para restablecer las estadísticas de las colas de software.

Sintaxis:

clear

Consulte el mandato **queue** para ver un ejemplo del mandato **clear**.

Queue

Utilice el mandato **queue** para mostrar las colas de software de los flujos de tráfico que no son ATM.

Sintaxis:

queue

La lista siguiente define los términos utilizados al visualizar las colas de software que no son ATM:

Quota

Cantidad de ancho de banda reservada. Originalmente, el tipo de mejor esfuerzo (B.E.) es el que tiene todas las cuotas. Cuando se realiza una reserva, el ancho de banda reservado (b/w) cambia de la cuota B.E. a la cuota QoS.

Max-q

Longitud máxima de cola, indicada en número de paquetes.

Curr-q

Longitud actual de la cola, indicada en número de paquetes.

In quota

Paquetes o kilobytes enviados en el ancho de banda asignado.

Outside quota

Paquetes o kilobytes enviados fuera del ancho de banda asignado, cuando había disponible un ancho de banda desocupado.

Packets/bytes dropped

Paquetes o bytes eliminados por el sistema de colas de software.

DLC packets/bytes dropped

Paquetes o bytes eliminados por DLC después de que los paquetes hayan atravesado la cola de software.

Ejemplo:

```
*t 5
```

```
+feature vcrm
VCRM console
VCRM Console>?
CLEAR
QUEUE
EXIT
```

```
VCRM Console>queue
```

```
Flow-control Queues at sys-clock 346781 Second:
```

```
-----
Intf  B.E. Quota:      10000 Kbps      QoS Quota:         0      Kbps
0/Eth  B.E. Max-q        0                QoS Max-q         0
      B.E. curr-q    0                QoS curr-q        0
      B.E. pkts/Kbytes sent:      QoS pkts/Kbytes sent:
      in quota:      54169/ 3926      in quota:         0/      0
      outside quota:  0/      0      outside quota:    0/      0
      B.E. pkts/bytes dropped: 0/0      QoS pkts/bytes dropped: 0/0
      DLC pkts/bytes dropped: B.E.: 0/0      QoS: 0/0
Intf  B.E. Quota:      2048 Kbps      QoS Quota:         0      Kbps
2/PPP  B.E. Max-q        0                QoS Max-q         0
      B.E. curr-q    0                QoS curr-q        0
      B.E. pkts/Kbytes sent:      QoS pkts/Kbytes sent:
      in quota:      62/      6      in quota:         0/      0
      outside quota:  0/      0      outside quota:    0/      0
      B.E. pkts/bytes dropped: 0/0      QoS pkts/bytes dropped: 0/0
      DLC pkts/bytes dropped: B.E.: 0/0      QoS: 0/0
Intf  B.E. Quota:      2032 Kbps      QoS Quota:        16      Kbps
3/FR   B.E. Max-q        1                QoS Max-q         1
      B.E. curr-q    0                QoS curr-q        0
      B.E. pkts/Kbytes sent:      QoS pkts/Kbytes sent:
      in quota:      53160/ 4920      in quota:      346596/ 31886
      outside quota:  0/      0      outside quota:    0/      0
      B.E. pkts/bytes dropped: 0/0      QoS pkts/bytes dropped: 0/0
      DLC pkts/bytes dropped: B.E.: 0/0      QoS: 0/0
Intf  B.E. Quota:      2048 Kbps      QoS Quota:         0      Kbps
4/PPP  B.E. Max-q        1                QoS Max-q         1
      B.E. curr-q    0                QoS curr-q        0
      B.E. pkts/Kbytes sent:      QoS pkts/Kbytes sent:
      in quota:      66/      6      in quota:      109/      1
      outside quota:  0/      0      outside quota:    0/      0
      B.E. pkts/bytes dropped: 0/0      QoS pkts/bytes dropped: 0/0
      DLC pkts/bytes dropped: B.E.: 0/0      QoS: 0/0
```

```
Max total queue length=1; current total length=0
```

```
VCRM Console>clear
```

```
Flow-control Queues cleared at sys-clock 346786 Second:
```

```
-----
VCRM Console>
```

Apéndice A. Atributos AAA remotos

Esta sección contiene los Atributos AAA remotos utilizados por los servidores Radius, TACACS y TACACS+.

Radius

ID proveedor IBM: 211

Atributos de autorización

Borrador estándar

TUNNEL_TYPE	64
TUNNEL_MEDIUM_TYPE	65
TUNNEL_CLIEN_TYPE	66
TUNNEL_SERVER_EP	67
TUNNEL_CONN_ID	68
TUNNEL_PASSWORD	69

valores

TUNNEL_TYPE		entero
3	L2TP	
TUNNEL_MEDIUM_TYPE		entero
1	IP	
TUNNEL_SERVER_EP		serie
	dirección IP	

Específico de proveedor IBM

NAS_TUNNEL_PASSWORD	101
CALLBACK_FLAGS	210
ENCRYPTION	211
HOSTNAME	213
SUBNETMASK	215
PRIVILEGE	216

Palabras clave

Se utilizan palabras clave para servidores Radius que permiten la entrada de campos específicos del proveedor <palabra clave>=<valor>.

KWD_CALLBACK_FLAGS	CBF
KWD_ENCRYPTION	ENC
KWD_HOSTNAME	HSN
KWD_SUBNETMASK	SNM
KWD_PRIVELGE	PRV

Valores

PRIVILEGE:
 ADMIN
 OPER
 MONITOR

CALLBACKFLAGS	
REQ	devolución llamada obli- gatoria
ROAM	devolución llamada itinerante

TACACS+

Autenticación

Autorización

PPP service=ppp protocol=ip
 LOGIN service=shell cmd=null pri_lvl*0

Atributos estándar de TACACS+

- service
- protocol
- cmd
- addr
- timeout
- priv_lvl
- callback-dialstring

Atributos específicos de IBM

encryption_key	16 caracteres hexadecimales
dial_out	TRUE FALSE ONLY

Contabilidad

- task_id
- start_time
- stop_time
- elapsed_time
- timezone
- event
- reason
- bytes
- bytes_in
- bytes_out
- paks

paks_in
paks_out
status
err_msg

Apéndice B. Lista de Abreviaturas

AARP	AppleTalk Address Resolution Protocol
ABR	Direccionador de marco de área
ack	Acuse de recibo
AIX	Advanced Interactive Executive
AMA	Direccionamiento MAC arbitrario
AMP	Supervisor presente activo
ANSI	American National Standards Institute
AP2	AppleTalk Phase 2
APPN	Advanced Peer-to-Peer Networking
ARE	Explorador de todas las rutas
ARI	Interfaz ATM real
ARI/FCI	Indicador de dirección reconocida/indicador de trama copiada
ARP	Address Resolution Protocol
AS	Sistema autónomo
ASBR	Direccionador de límite de sistema autónomo
ASCII	American National Standard Code for Information Interchange
ASN.1	Notación de sintaxis de abstracción 1
ASRT	Direccionamiento transparente de origen adaptable
ASYNC	Asíncrono
ATCP	AppleTalk Control Protocol
ATP	AppleTalk Transaction Protocol
AUI	Interfaz de unidad de conexión
AVI	Interfaz ATM virtual
ayt	¿Hay alguien ahí?
BAN	Boundary Access Node
BBCM	Bridging Broadcast Manager
BECN	Notificación de congestión explícita hacia atrás
BGP	Border Gateway Protocol
BNC	Bayonet Niell-Concelman
BNCP	Bridging Network Control Protocol
BOOTP	Protocolo BOOT
BPDU	Unidad de datos de protocolo de puente
bps	Bits por segundo
BR	Función de puente/direccionamiento

BRS	Reserva de ancho de banda
BSD	Distribución de software de Berkeley
BTP	Agente de relay de BOOTP
BTU	Unidad básica de transmisión
CAM	Memoria dirigible a través del contenido
CCITT	Comisión Consultiva de la Telefonía y Telegrafía Internacionales
CD	Detección de colisión
CGWCON	Consola de pasarela
CIDR	Direccionamiento entre dominios sin clase
CIP	Classical IP
CIR	Velocidad de información comprometida
CLNP	Connectionless-Mode Network Protocol
CPU	Unidad central de proceso
CRC	Comprobación de redundancia cíclica
CRS	Servidor de informes de configuración
CTS	Preparado para transmitir
CUD	Datos de usuario de llamada
DAF	Filtración de direcciones de destino
DB	Base de datos
DBsum	Resumen de la base de datos
DCD	Detector de señal de línea recibida de canal de datos
DCE	Equipo de terminación de circuito de datos
DCS	Servidor conectado directamente
DDLC	Controlador de enlace de datos dual
DDN	Defense Data Network
DDP	Datagram Delivery Protocol
DDT	Dynamic Debugging Tool
DHCP	Dynamic Host Configuration Protocol
dir	Conectado directamente
DL	Enlace de datos
DLC	Control de enlace de datos
DLCI	Identificador de conexión de enlace de datos
DLS	Conmutación del enlace de datos
DLSw	Conmutación del enlace de datos
DMA	Acceso de memoria directo
DNA	Digital Network Architecture
DNCP	DECnet Protocol Control Protocol

DNIC	Código de identificador de red de datos
DdD	Departamento de Defensa
DOS	Disk Operating System
DR	Direccionador designado
DRAM	Memoria de acceso aleatorio dinámica
DSAP	Punto de acceso a servicios de destino
DSE	Equipo de conmutación de datos
DSE	Intercambio de conmutaciones de datos
DSR	Aparato de datos preparado
DSU	Unidad de servicio de datos
DTE	Equipo terminal de datos
DTR	Terminal de datos preparado
Dtype	Tipo de destino
DVMRP	Distance Vector Multicast Routing Protocol
E1	Velocidad de transmisión de 2,048 Mbps
EDEL	Delimitador de final
EDI	Indicador de errores detectados
EGP	Exterior Gateway Protocol
EIA	Electronics Industries Association
ELAN	LAN emulada
ELAP	EtherTalk Link Access Protocol
ELS	Sistema de anotación cronológica de sucesos
ELSCon	Consola secundaria de ELS
ESI	Identificador de sistema final
EST	Horario Estándar del Este de los EE.UU
Eth	Ethernet
fa-ga	Dirección funcional-dirección de grupo
FCS	Secuencia de comprobación de trama
FECN	Notificación de congestión explícita hacia adelante
FIFO	Primero en entrar, primero en salir
FLT	Biblioteca de filtros
FR	Frame Relay
FRL	Frame Relay
FTP	File Transfer Protocol
GMT	Hora Media de Greenwich
GOSIP	Perfil de Interconexión de Sistemas Abiertos del Gobierno
GTE	Compañía Telefónica General

GWCON	Consola de pasarela
HDLC	Control de enlace de datos de alto nivel
HEX	Hexadecimal
HPR	Direccionamiento de alto rendimiento
HST	Servicios de sistema principal de TCP/IP
HTF	Formato de tabla de sistema principal
IBD	Dispositivo de arranque integrado
ICMP	Internet Control Message Protocol
ICP	Internet Control Protocol
ID	Identificación
IDP	Parte de dominio inicial
IDP	Internet Datagram Protocol
IEEE	Institute of Electrical and Electronics Engineers
Ifc#	Número de interfaz
IGP	Interior Gateway Protocol
InARP	Inverse Address Resolution Protocol
IP	Internet Protocol
IPCP	IP Control Protocol
IPPN	IP Protocol Network
IPX	Internetwork Packet Exchange
IPXCP	IPX Control Protocol
RDSI	Red digital de servicios integrados
ISO	Organización Internacional para la Normalización
Kbps	Kilobits por segundo
LAC	Concentrador del acceso a la red L2TP
LAN	Red de área local
LAPB	Protocolo de acceso a enlace equilibrado
LAT	Transporte de área local
LCS	Estación de canal de LAN
LCP	Link Control Protocol
LED	Diodo emisor de luz
LF	Trama mayor; salto de línea
LIS	Subred IP lógica
LLC	Control de enlace lógico
LLC2	Control de enlace lógico 2
LMI	Interfaz de gestión local
LNS	Servidor de red L2TP

LRM	Mecanismo de información de LAN
LS	Estado de los enlaces
LSA	Notificación del estado de los enlaces
LSA	Link Services Architecture
LSB	Bit menos significativo
LSI	Interfaz de métodos abreviados de LAN
LSreq	Petición del estado de los enlaces
LSrxl	Lista de retransmisiones del estado de los enlaces
LU	Unidad lógica
MAC	Control del acceso al medio
Mb	Megabit
MB	Megabyte
Mbps	Megabits por segundo
MBps	Megabytes por segundo
MC	Multidifusión
MCF	Filtración MAC
MIB	Base de la información de gestión
MIB II	Base de la información de gestión II
MILNET	Red militar
MOS	Micro Operating System
MOSDBG	Micro Operating System Debugging Tool
MOSPF	Open Shortest Path First con extensiones de multidifusión
MPC	Canal de diversas vías de acceso
MPC+	Canal de diversas vías de acceso de transferencia de datos de alto rendimiento (HPDT)
MSB	Bit más significativo
MSDU	Unidad de datos de servicio MAC
MRU	Unidad máxima de recepción
MTU	Unidad máxima de transmisión
nak	Sin acuse de recibo
NAS	Estación Nways Switch Administration
NBMA	Acceso múltiple sin difusión
NBP	Name Binding Protocol
NBR	Direccionador contiguo
NCP	Network Control Protocol
NCP	Network Core Protocol
NDPS	Conmutación de vías de acceso sin interrupciones

NetBIOS	Network Basic Input/Output System
NHRP	Next Hop Resolution Protocol
NIST	National Institute of Standards and Technology
NPDU	Unidad de datos de protocolo de red
NRZ	Sin vuelta a cero
NRZI	Sin vuelta a cero invertido
NSAP	Punto de acceso a servicios de red
NSF	National Science Foundation
NSFNET	National Science Foundation NETwork
NVCNFG	Configuración permanente
OPCON	Consola del operador
OSI	Interconexión de sistemas abiertos
OSICP	OSI Control Protocol
OSPF	Open Shortest Path First
OUI	Identificador exclusivo de organización
PC	Personal Computer
PCA	Adaptador de canal paralelo
PCR	Velocidad punta 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	Petición de emisión
Rtype	Tipo de ruta
rxmits	Retransmisiones
rxmt	Retransmisión
s	Segundo
SAF	Filtración de direcciones de origen
SAP	Punto de acceso a servicios
SAP	Service Advertising Protocol
SCR	Velocidad sostenida de célula
SCSP	Server Cache Synchronization Protocol
sdel	Delimitador de inicio
SDLC	Relay de SDLC, control síncrono de enlace de datos
seqno	Número de secuencia
SGID	Identificación de grupo de servidores
SGMP	Simple Gateway Monitoring Protocol
SL	Línea serie
SMP	Supervisor presente en espera
SMTP	Simple Mail Transfer Protocol
SNA	Systems Network Architecture
SNAP	Subnetwork Access Protocol
SNMP	Simple Network Management Protocol
SNPA	Punto de conexión de subred
SPF	Ruta intraárea OSPF
SPE1	Tipo 1 de ruta externa OSPF
SPE2	Tipo 2 de ruta externa OSPF
SPIA	Tipo de ruta interárea OSPF
SPID	Identificación de perfil de servicio
SPX	Sequenced Packet Exchange
SQE	Error en calidad de señal
SRAM	Memoria de acceso aleatorio estática
SRB	Puente de direccionamiento de origen

SRF	Trama específicamente direccionada
SRLY	Relay de SDLC
SRT	Direccionamiento transparente de origen
SR-TB	Puente de direccionamiento transparente de origen
STA	Estático
STB	Puente de árbol de expansión
STE	Explorador de árbol de expansión
STP	Par trenzado y apantallado; protocolo de árbol de expansión
SVC	Circuito virtual conmutado
TB	Puente transparente
TCN	Notificación de cambio de topología
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TEI	Identificador de punto de terminal
TFTP	Trivial File Transfer Protocol
TKR	Red en Anillo
TMO	Tiempo de espera excedido
TOS	Tipo de servicio
TSF	Tramas de expansión transparentes
TTL	Período de duración
TTY	Teletipo
TX	Transmisión
UA	Acuse de recibo sin número
UDP	User Datagram Protocol
UI	Información sin número
UTP	Par trenzado y no apantallado
VCC	Conexión de canal virtual
VINES	Virtual NETworking System
VIR	Velocidad de información variable
VL	Enlace virtual
VNI	Virtual Network Interface
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 *Fiber Optic Terminology*, ANSI/EIA norma—440-A. 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 anterior 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. 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.

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.

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 petición y respuesta de cliente/servidor a los sistemas principales que acceden al protocolo Zone Information Protocol (ZIP) para la información de zonas.

árbol de expansión. En contextos de LAN, método mediante el cual los puentes desarrollan automáticamente una tabla de direccionamiento y actualizan esta tabla en respuesta a un cambio de la topología para asegurarse de la existencia de una sola ruta entre dos LAN cualesquiera en la red con puentes. Este método evita bucles de paquetes, donde un paquete vuelve en una ruta de circuito al direccionador emisor.

archivo de configuración. Archivo que especifica las características de un dispositivo del sistema o una red.

área. En los protocolos de direccionamiento de Internet y DECnet, subconjunto de una red o pasarela que se ha agrupado por definición del administrador de red. Cada área es independiente; la información sobre la topología de un área permanece oculta respecto a las otras áreas.

arquitectura de red. Estructura lógica y principios operativos de una red de sistema. (T)

Nota: Los principios operativos de una red incluyen los principios de los servicios, funciones y protocolos.

arquitectura Interconexión de Sistemas Abiertos (OSI). Arquitectura de red que se ajusta al conjunto particular de normas ISO relacionado con Interconexión de Sistemas Abiertos. (T)

arreglo temporal del programa (PTF). Solución o ajuste temporal de un problema diagnosticado por IBM del release actual no modificado del programa.

asequibilidad. Capacidad de un nodo o recurso para comunicarse con otro nodo o recurso.

asíncrono (ASYN). Perteneciente a dos o más procesos que no dependen de la aparición de sucesos específicos, como, por ejemplo, señales comunes de temporización. (T)

ATM. Asynchronous Transfer Mode, tecnología de red de gran velocidad orientada a las conexiones que se basa en la conmutación de células.

ATMARP. ARP en Classical IP.

B

base de datos de configuración (CDB). Base de datos que almacena los parámetros de configuración de uno o diversos dispositivos. Se prepara y actualiza utilizando el programa de configuración.

Base de la información de gestión (MIB). (1) Conjunto de objetos a los que se puede acceder por medio de un protocolo de gestión de red. (2) Definición de información de gestión que especifica la información disponible de un sistema principal o una pasarela y las operaciones permitidas. (3) En OSI, depósito conceptual de información de gestión dentro de un sistema abierto.

baudio. En la transmisión asíncrona, unidad de velocidad de modulación correspondiente al intervalo de una unidad por segundo; es decir, si la duración del intervalo de la unidad es de 20 milisegundos, la velocidad de modulación es de 50 baudios. (A)

bit D. Bit de confirmación de entrega. En comunicaciones X.25, bit de un paquete de datos o paquete de petición de llamada que se establece en 1 si el destinatario necesita acuse de recibo (confirmación de entrega) de final a final.

Border Gateway Protocol (BGP). Protocolo de direccionamiento Internet Protocol (IP) utilizado entre dominios y sistemas autónomos.

bucle de direccionamiento. Situación que ocurre cuando los direccionadores hacen circular información entre ellos hasta que se produce la convergencia o hasta que se consideran inasequibles las redes implicadas.

C

cabecera. (1) Información de control definida por el sistema que precede a los datos de usuario. (2) Parte de un mensaje que contiene información de control para el mismo, como, por ejemplo, uno o más campos de destino, el nombre de la estación de origen, el número de secuencia de entrada, una serie de caracteres que indica el tipo de mensaje y el nivel de prioridad del mensaje.

cabecera de transmisión (TH). Información de control, seguida opcionalmente de una unidad básica de información (BIU) o de un segmento de BIU, que crea y utiliza el control de la vía de acceso para direccionar unidades de mensajes y controlar su flujo dentro de la red. Véase también *unidad de información de vía de acceso*.

canal. (1) Vía de acceso por la que pueden enviarse señales, como, por ejemplo, canal de datos, canal de salida. (A) (2) Unidad funcional, controlada por el procesador, que maneja la transferencia de datos entre el almacenamiento del procesador y el equipo de periféricos local.

canal de diversas vías de acceso (MPC). Protocolo de canal que utiliza diversos subcanales unidireccionales para la comunicación bidireccional de VTAM a VTAM.

canal de entrada/salida. En un sistema de proceso de datos, unidad funcional que maneja la transferencia de datos entre el equipo interno y el equipo de periféricos. (I) (A)

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.

canalización. Proceso consistente en romper el ancho de banda de una línea de comunicaciones en varios canales, posiblemente de diferentes tamaños. También se denomina *multiplexación de la división del tiempo* (TDM).

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 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 final a final. Puede haber sistemas abiertos 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 a y de 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 la Emulación de LAN (LEC). Componente de Emulación de LAN que representa a los usuarios de la LAN emulada.

cliente/servidor. En comunicaciones, modelo de interacción en el proceso de datos distribuidos en el que un programa de un sitio envía una petición a un programa de otro sitio y espera una respuesta. El programa peticionario se denomina cliente; el programa que responde se denomina servidor.

codificar. Convertir datos mediante el uso de un código de manera que sea posible la reconversión al formato original. (T)

colisión. Condición no deseada que deriva de la existencia de transmisiones simultáneas en un canal. (T)

compresión. (1) Proceso consistente en eliminar claros, campos vacíos, redundancias y datos innecesarios para disminuir la longitud de los registros o los bloques. (2) Cualquier codificación destinada a reducir el número de bits utilizados para representar un mensaje o un registro determinado.

comunidad. En el protocolo Simple Network Management Protocol (SNMP), relación administrativa entre las entidades.

concentrador (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.

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.

conectable en caliente. Se refiere a un componente de hardware que puede instalarse o eliminarse sin estorbar el funcionamiento de otros recursos que no están conectados a este componente o no dependen del mismo.

conectado mediante enlace. (1) Perteneciente a dispositivos que están conectados a una unidad de control por medio de un enlace de datos. (2) Compárese con *conectado mediante canal*. (3) Sinónimo con *remoto*.

conexión. En la comunicación de datos, asociación establecida entre unidades funcionales para comunicar información. (I) (A)

conexión de enlace. (1) Equipo físico que proporciona comunicación en dos direcciones entre una estación de enlace y otra u otras estaciones de enlace; por ejemplo, un equipo de terminación de circuito de datos (DCE) y una línea de telecomunicaciones. (2) En SNA, sinonimia con *circuito de datos*.

conexión Rapid Transport Protocol (RTP). En el direccionamiento de alto rendimiento (HPR), conexión establecida entre los puntos finales de la ruta para transportar tráfico de sesión.

conexión virtual. En frame relay, vía de acceso de vuelta de una conexión potencial.

configuración. (1) Manera en que están organizados e interconectados el hardware y el software de un sistema de proceso de información. (T) (2) Dispositivos y programas que componen un sistema, un subsistema o una red.

configuración del sistema. Proceso que especifica los dispositivos y programas que componen un sistema de proceso de datos determinado.

congestión. Véase *congestión de la red*.

congestión de la red. Condición no deseada de carga excesiva causada por la presencia de más tráfico del que puede manejar una red.

conmutación de la línea. Sinónimo de *conmutación del circuito*.

conmutación de paquetes. (1) Proceso consistente en direccionar y transferir datos por medio de paquetes dirigidos de manera que un canal esté ocupado durante la transmisión de un paquete solamente. Cuando se

completa la transmisión, el canal queda disponible para la transferencia de otros paquetes. (1) (2) Sinónimo con *funcionamiento en modalidad de paquete*. Véase también *conmutación del circuito*.

conmutación del circuito. (1) Proceso que, a petición, conecta dos o más equipos terminales de datos (DTE) y permite el uso exclusivo de un circuito de datos entre ellos hasta que se libera la conexión. (1) (A) (2) Sinónimo con *conmutación de la línea*.

conmutación del enlace de datos (DLSw). Método para transportar protocolos de red que utilizan el tipo 2 de control de enlace lógico (LLC) de IEEE 802.2. SNA y NetBIOS son ejemplos de protocolos que utilizan el tipo 2 de LLC. Véase también *encapsulación y simulación*.

consola remota. Estación que ejecuta OS/2, TCP/IP y el programa Nways Switch Resource Control remoto. Puede conectarse con cualquier estación de soporte de red para realizar operaciones en Nways Switch y darle servicio técnico remotamente.

La conexión puede ser mediante:

- Una línea conmutada que utilice un módem

Cualquier estación de soporte de red puede utilizarse como consola remota de otra estación de soporte de red.

contigua activa de donde proceden los datos (NAUN). En la Red en Anillo de IBM, estación que envía datos directamente a una estación determinada del anillo.

control de enlace de datos (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 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 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 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 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 MAC incluye el método para determinar cuándo un dispositivo tiene acceso al medio de transmisión.

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 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 pasar en la vía de acceso a un destino.

D

daemon. Programa que se ejecuta desatendido para realizar un servicio estándar. Algunos daemons se desencadenan de manera automática para realizar su tarea; otros realizan las operaciones periódicamente.

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.

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.

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 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 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 portadora. En una red de área local, actividad continua de una estación de datos para detectar si otra estación está transmitiendo. (T)

detector de portadora. Sinónimo de *detector de señal de línea recibida (RLSD)*.

detector de portadora de datos (DCD). Sinónimo de *detector de señal de línea recibida (RLSD)*.

detector de señal de línea recibida (RLSD). En la norma EIA 232, señal que indica al equipo terminal de datos (DTE) que está recibiendo una señal del equipo de terminación de circuito de datos (DCE) remoto. Sinónimo con *detector de portadora* y *detector de portadora de datos (DCD)*.

determinación de problemas. Proceso consistente en determinar el origen de un problema; por ejemplo, un componente de un programa, una anomalía en una máquina, recursos de telecomunicaciones, programas o equipos instalados por el contratista o por el usuario, una anomalía del entorno, como, por ejemplo, pérdida de alimentación, o un error del usuario.

difusión. (1) Transmisión de los mismos datos a todos los destinos. (T) (2) Transmisión simultánea de datos a más de un destino. (3) Compárese con *multidifusión*.

digital. (1) Perteneciente a datos compuestos por dígitos. (T) (2) Perteneciente a datos con formato de dígitos. (A) (3) Compárese con *analógico*.

Digital Network Architecture (DNA). Modelo para todas las implementaciones de hardware y software DECnet.

dirección. En la comunicación de datos, código exclusivo asignado a cada dispositivo, estación de trabajo o usuario conectado a una red.

dirección administrada localmente. En una red de área local, dirección de adaptador que el usuario puede asignar para alterar temporalmente la dirección administrada universalmente. Compárese con *dirección administrada universalmente*.

dirección administrada universalmente. En una red de área local, dirección codificada de forma permanente en un adaptador en el momento de la fabricación. Todas las direcciones administradas universalmente son exclusivas. Compárese con *dirección administrada localmente*.

dirección canónica. En las LAN, formato de IEEE 802.1 de la transmisión de direcciones del control del acceso al medio (MAC) para adaptadores de Red en Anillo y Ethernet. En el formato canónico, el bit menos significativo (situado más a la derecha) de cada byte de dirección se transmite en primer lugar. Compárese con *dirección no canónica*.

dirección de difusión. En comunicaciones, dirección de estación (ocho números 1) reservada como dirección común a todas las estaciones de un enlace. Sinónimo con *dirección de todas las estaciones*.

dirección de dispositivo. Dirección de unidad transmitida por la vía de acceso de canal para seleccionar un dispositivo 2216. También se denomina número de subcanal en la arquitectura de E/S S/370. Este valor está definido en el IOCP del sistema principal mediante la sentencia UNITADD de la instrucción de macro CNTLUNIT para el dispositivo real.

Dirección de enlace. Para el 2216 con un Adaptador de Canal ESCON, número de puerto determinado de la manera siguiente: si hay un ESCD en la vía de acceso de comunicaciones, es el número de puerto del Director de ESCON (ESCD) conectado al sistema principal. Si hay dos ESCD en la vía de acceso, es el número de puerto de la parte del sistema principal del ESCD definido con la conexión dinámica. Cuando no hay ningún ESCD en la vía de acceso de comunicaciones, este valor debe establecerse en X'01'.

dirección de red. Según ISO 7498-3, nombre que no es ambiguo en el entorno de OSI y que identifica a un conjunto de puntos de acceso a servicios de red.

dirección de subred. En comunicaciones de Internet, extensión del esquema básico de direccionamiento de IP donde una parte de la dirección de sistema principal se interpreta como dirección de red local.

dirección de todas las estaciones. En comunicaciones, sinónimo de *dirección de difusión*.

dirección de usuario de red (NUA). En comunicaciones de X.25, dirección X.121 que contiene hasta 15 dígitos en código binario.

dirección Internet. Véase *dirección IP*.

dirección IP. Dirección de 32 bits definida por Internet Protocol, norma 5, Request for Comments (RFC) 791. Normalmente, se representa mediante notación decimal con puntos.

Dirección lógica de CU. Dirección de unidad de control definida en el sistema principal para el 2216. Este valor está definido en el programa de configuración de la entrada/salida (IOCP) del sistema principal mediante la sentencia CUADD de la instrucción de macro CNTLUNIT. La Dirección de unidad de control debe ser exclusiva para cada partición lógica definida en el mismo sistema principal.

dirección no canónica. En las LAN, formato de la transmisión de direcciones del control del acceso al medio (MAC) para adaptadores de Red en Anillo. En el formato no canónico, el bit más significativo (situado más a la izquierda) de cada byte de dirección se transmite en primer lugar. Compárese con *dirección canónica*.

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 ini-

cialmente 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. (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. En la comunicación de datos, manera que tiene una estación de seleccionar la estación a la que va a enviar datos.

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 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.

direccionamiento 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.

directorio. 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 sistemas en la que los recursos de proceso de datos están bajo un control común. (T) (2) En Interconexión de Sistemas Abiertos (OSI), parte de un sistema distribuido o conjunto de objetos gestionados a los que se aplica una política común. (3) Véase *Dominio administrativo* y *nombre de dominio*.

Dominio administrativo. Conjunto de sistemas principales y direccionadores, y las redes de interconexión, que gestiona una sola autoridad administrativa.

dominio de direccionamiento. En comunicaciones de Internet, grupo de sistemas intermedios que utilizan un protocolo de direccionamiento para que la representación de la red en un conjunto sea la misma en cada sistema intermedio. Los dominios de direccionamiento se conectan entre sí mediante enlaces exteriores.

E

eco. En la comunicación de datos, señal de un canal de comunicaciones reflejada. Por ejemplo, en un terminal de comunicaciones, cada señal se visualiza dos veces, una cuando entra en el terminal local y otra cuando vuelve sobre el enlace de comunicaciones. Esto permite comprobar la exactitud de las señales.

EIA 232. En la comunicación de datos, especificación de la Electronic Industries Association (EIA) que define la interfaz entre el equipo terminal de datos (DTE) y el equipo de terminación de circuito de datos (DCE), que utiliza el intercambio de datos binarios serie.

Electronic Industries Association (EIA). Organización de fabricantes del campo de la electrónica que anticipa el crecimiento tecnológico de la industria,

representa los puntos de vista de sus miembros y desarrolla normas para la industria.

Emulación de LAN (LE). Norma del ATM Forum que da soporte a aplicaciones de legado de LAN sobre redes ATM.

encapsulación. (1) En comunicaciones, técnica utilizada por protocolos de capa mediante la cual una capa añade a la unidad de datos de protocolo (PDU) información de control de la capa a la que da soporte. A este respecto, la capa encapsula los datos de la capa soportada. En el conjunto de protocolos de Internet, por ejemplo, un paquete contendrá información de control de la capa física, a continuación información de control de la capa de red y a continuación los datos de protocolo de la aplicación. (2) Véase también *conmutación del enlace de datos*.

enlace. Combinación de la conexión de enlace (el medio de transmisión) y dos estaciones de enlace, una a cada extremo de la conexión de enlace. Una conexión de enlace puede estar compartida entre diversos enlaces en una configuración de multipunto o Red en Anillo.

enlace lógico. Par de estaciones de enlace, una en cada uno de dos nodos adyacentes, y su conexión de enlace subyacente que proporcionan una sola conexión de capa de enlace entre los dos nodos. Pueden distinguirse diversos enlaces lógicos mientras comparten el uso del mismo medio físico de conexión de dos nodos. Ejemplos son los enlaces lógicos de 802.2 utilizados en recursos de red de área local (LAN) y los enlaces lógicos de LAP E del mismo enlace físico punto a punto entre dos nodos. El término enlace lógico también incluye los diversos canales lógicos de X.25 que comparten el uso del enlace de acceso de un DTE con una red X.25.

enlace virtual. En Open Shortest Path First (OSPF), interfaz punto a punto que conecta direccionadores de frontera separados por un área de tránsito no troncal. Puesto que los direccionadores de área forman parte del troncal OSPF, el enlace virtual conecta el troncal. Los enlaces virtuales aseguran que el troncal OSPF no se vuelva discontinuo.

equipo de terminación de circuito de datos (DCE). En una estación de datos, equipo que proporciona la conversión de señal y la codificación entre el equipo terminal de datos (DTE) y la línea. (I)

Notas:

1. El DCE puede ser un equipo independiente o parte integral del DTE o del equipo intermedio.
2. Un DCE puede realizar otras funciones que normalmente se llevan a cabo al final de red de la línea.

equipo terminal de datos (DTE). Parte de una estación de datos que funciona como origen y/o destino de datos. (I) (A)

esfera de control (SOC). Conjunto de dominios de punto de control servidos por un solo punto focal de servicios de gestión.

estación. Punto de entrada o salida de un sistema que utiliza recursos de telecomunicaciones; por ejemplo, uno o más sistemas, terminales, dispositivos y programas asociados de una ubicación determinada que pueden enviar o recibir datos sobre una línea de telecomunicaciones.

estación de configuración Nways Switch. Estación de OS/2 dedicada que ejecuta una versión autónoma de la herramienta Nways Switch Configuration Tool (NCT). Se utiliza para generar una base de datos de configuración de red y debe instalarse como consola remota.

estación de enlace. (1) Componentes de hardware y software de un nodo que representan una conexión con un nodo adyacente sobre un enlace específico. Por ejemplo, si el nodo A es el extremo primario de una línea multipunto que se conecta con tres nodos adyacentes, el nodo A tendrá tres estaciones de enlace que representarán las conexiones con los nodos adyacentes. (2) Véase también *estación de enlace adyacente (ALS)*.

estación de gestión. En comunicaciones de Internet, sistema responsable de la gestión de toda una red o de parte de la misma. La estación de gestión se comunica con agentes de gestión de red que residen en el nodo gestionado por medio de un protocolo de gestión de red, como, por ejemplo, Simple Network Management Protocol (SNMP).

estación de gestión de red. En el protocolo Simple Network Management Protocol (SNMP), estación que ejecuta programas de aplicación de gestión que supervisan y controlan elementos de red.

estación de soporte de red. Procesador utilizado para realizar operaciones en Nways Switch y darle servicio técnico localmente. Lo utilizan el administrador o el personal de servicio encargados de Nways Switch.

estado de los enlaces. En los protocolos de direccionamiento, información anunciada sobre las interfaces utilizables y los direccionadores contiguos a un direccionador o una red asequibles. La base de datos topológica del protocolo se forma a partir de los anuncios reunidos sobre el estado de los enlaces.

Estructura de la información de gestión (SMI). (1) En el protocolo Simple Network Management Protocol (SNMP), normas utilizadas para definir los

objetos a los que puede accederse por medio de un protocolo de gestión de red. (2) En OSI, conjunto de normas relativas a la información de gestión. El conjunto incluye el *Management Information Model* y las *Guidelines for the Definition of Managed Objects*.

Ethernet. Red de área local de banda base de 10 Mbps que permite que diversas estaciones accedan al medio de transmisión a voluntad sin coordinación previa, evita la contención utilizando la detección y deferencia de portadora y resuelve la contención utilizando la detección de colisión y la retransmisión retardada. Ethernet utiliza el acceso múltiple con detección de portadora y detección de colisión (CSMA/CD).

excepción. Condición anormal, como, por ejemplo, un error de E/S encontrado durante el proceso de un conjunto de datos o archivo.

extensión de ruta (REX). En SNA, componentes de red de control de la vía de acceso, incluido un enlace periférico, que componen la parte de una vía de acceso que está entre un nodo de subárea y una unidad de red direccionable (NAU) de un nodo periférico adyacente. Véase también *ruta explícita (ER)*, *vía de acceso y ruta virtual (VR)*.

Exterior Gateway Protocol (EGP). En el conjunto de protocolos de Internet, protocolo utilizado entre dominios y sistemas autónomos que permite anunciar e intercambiar información sobre la asequibilidad de la red. Las direcciones de red IP de un sistema autónomo se anuncian en otro sistema autónomo por medio de direccionadores que participan de EGP. Un ejemplo de EGP es Border Gateway Protocol (BGP). Compárese con Interior Gateway Protocol (IGP).

F

fax. Copia impresa que se recibe de una máquina de facsímil. Sinónimo con *telecopia*.

File Transfer Protocol (FTP). En el conjunto de protocolos de Internet, protocolo de capa de aplicación que utiliza servicios de TCP y Telnet para transferir archivos de datos generales entre máquinas o sistemas principales.

fluctuación. (1) Variaciones no acumulativas a corto plazo de los instantes significativos de una señal digital respecto a sus posiciones ideales en el tiempo. (2) Variaciones no deseadas de una señal digital transmitida. (3) Variaciones en el retardo de la red.

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 tiene lugar de final a final 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.

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 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 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*.

funcionamiento en modalidad de paquete. Sinónimo de *conmutación de paquetes*.

G

gestión de red. Proceso consistente en planificar, organizar y controlar un proceso de datos o sistema de información orientado a las comunicaciones.

gestor de red. Programa o grupo de programas que se utiliza para supervisar y gestionar una red así como para diagnosticar los problemas de la misma.

grupo de transmisión (TG). (1) Conexión entre nodos adyacentes que se identifica mediante un número de grupo de transmisión. (2) En una red de subárea, enlace o grupo de enlaces entre nodos adyacentes. Cuando un grupo de transmisión está compuesto por un grupo de enlaces, los enlaces se ven como un solo enlace lógico y el grupo de transmisión se denomina *grupo de transmisión multienlace (MLTG)*. Un *grupo de transmisión multienlace de mezcla de medios (MMMLTG)* contiene enlaces de diferentes tipos de medios (por ejemplo, Red en Anillo, SDLC conmutado, SDLC no conmutado y enlaces frame-relay). (3) En una red APPN, enlace entre nodos adyacentes. (4) Véase también *grupos de transmisión paralelo*.

grupos de transmisión paralelo. Diversos grupos de transmisión entre nodos adyacentes, teniendo cada grupo un número de grupo de transmisión distinto.

H

Hello. Protocolo utilizado por un grupo de direccionadores que cooperan y se apoyan entre sí para poder descubrir rutas de retardo mínimo.

heurístico. Perteneciente a métodos exploratorios para la resolución de problemas en los que se descubren soluciones mediante una evaluación del progreso realizada respecto al resultado final.

histéresis. Cantidad que indica cuánto debe cambiar la temperatura una vez pasado el umbral del establecimiento de alerta y antes de que se elimine la condición de alerta.

horizonte dividido. Técnica destinada a minimizar el tiempo para conseguir la convergencia en la red. Un direccionador registra la interfaz sobre la que ha recibido una ruta en particular y no propaga su información sobre la ruta otra vez sobre la misma interfaz.

I

identificación de intercambio (XID). Tipo específico de unidad básica de enlace que se utiliza para la comunicación de características de nodo y enlace entre nodos adyacentes. Los XID se intercambian entre estaciones de enlace antes de la activación del enlace

y durante la misma para establecer y negociar las características de enlace y nodo, y después de la activación del enlace para comunicar los cambios de estas características.

identificador de conexión de enlace de datos (DLCI). Identificador numérico de un subpuerto frame-relay o segmento de PVC en una red frame-relay. Cada subpuerto de un puerto frame-relay individual tiene un DLCI exclusivo. La tabla siguiente, extraída de la norma T1.618 del American National Standards Institute (ANSI) y la norma Q.922 de la Comisión Consultiva de la Telefonía y Telegrafía Internacionales (ITU-T/CCITT), indica las funciones asociadas con determinados valores de DLCI:

Valores de DLCI	Función
0	señalización de canal de entrada
1–15	se reserva
16–991	se asigna utilizando procedimientos de conexión de frame-relay
992–1007	gestión de capa 2 de servicio 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 abajo 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 ID 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) Utilización de procedimientos normalizados para permitir la interconexión de sistemas de proceso de datos.

Nota: La arquitectura OSI establece una infraestructura para coordinar el desarrollo de normas actuales y futuras de cara a la interconexión de sistemas. Las funciones de red se dividen en siete capas. Cada capa representa un grupo de funciones relacionadas de proceso de datos y comunicación que pueden llevarse a cabo de una manera estándar para dar soporte a diferentes aplicaciones.

interfaz. (1) Límite compartido entre dos unidades funcionales en cuya definición entran características funcionales, características de señalización u otras características según lo que corresponda. El concepto incluye la especificación de la conexión de dos dispositivos que tienen funciones diferentes. (T)

(2) Hardware y/o software para el enlace de sistemas, programas o dispositivos.

interfaz de gestión local (LMI). Véase *protocolo de interfaz de gestión local (LMI)*.

interfaz de unidad de conexión (AUI). En una red de área local, interfaz entre la unidad de conexión al medio y el equipo terminal de datos de una estación de datos. (I) (A)

Interior Gateway Protocol (IGP). En el conjunto de protocolos de Internet, protocolo utilizado para propagar información sobre la asequibilidad y direccionamiento de la red dentro de un sistema autónomo. Ejemplos de IGP son Routing Information Protocol (RIP) y Open Shortest Path First (OSPF).

Internet. 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. Conjunto de redes interconectadas por una serie de direccionadores que les permiten funcionar como una sola red grande. Véase también *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)

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.

línea tronco. Línea de gran velocidad que conecta dos Nways Switch. Puede ser un cable coaxial, un cable de fibra u ondas de radio, por ejemplo, y puede alquilarse en empresas de telecomunicación.

local. (1) Perteneciente a un dispositivo al que se accede directamente sin utilizar una línea de telecomunicaciones. (2) Compárese con *remoto*. (3) Sinónimo de *conectado mediante canal*.

LP. partición lógica

LPAR. lógicamente particionada

M

mandato ping. Mandato que envía un paquete de petición con eco de Internet Control Message Protocol (ICMP) a una pasarela, direccionador o sistema principal esperando recibir una respuesta.

máscara. (1) Patrón de caracteres utilizado para controlar la retención o eliminación de partes de otro patrón de caracteres. (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.

modalidad lógicamente particionada (LPAR). Función de algunos procesadores principales en que el proceso se divide en particiones lógicas (LP) para parecer diversos procesadores. En modalidad LPAR, el adaptador de ESCON puede compartir una conexión de fibra física con diversas particiones de sistema principal.

modalidad LPAR. Modalidad lógicamente particionada (LPAR).

modelo de referencia Interconexión de Sistemas Abiertos (OSI). Modelo que describe los principios generales de Interconexión de Sistemas Abiertos así

como la finalidad y la ordenación jerárquica de sus siete capas. (T)

módem (modulador/demodulador). (1) Unidad funcional que modula y demodula señales. Una de las funciones de un módem es permitir que los datos digitales se transmitan sobre recursos de transmisión analógicos. (T) (A) (2) Dispositivo que convierte los datos digitales de un sistema en una señal analógica que pueda transmitirse en una línea de telecomunicaciones, y convierte la señal analógica recibida en datos para el sistema.

modulación en código de pulsaciones (PCM).

Norma adoptada para la digitalización de una señal de voz analógica. En la PCM, se realiza un muestreo de la voz a una velocidad de ocho kHz y cada muestra se codifica en una trama de 8 bits.

módulo. En Nways Switch, unidad de hardware funcional empaquetada que contiene tarjetas lógicas, conectores y luces. Los módulos se utilizan para empaquetar adaptadores, acopladores de interfaz de línea, extensiones de servidor de voz y otros componentes. Todos los módulos pueden **conectarse en caliente** en los subastidores lógicos.

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).

multiplexación de la división del tiempo (TDM). Véase *canalización*.

N

Name Binding Protocol (NBP). En redes AppleTalk, protocolo que proporciona la función de conversión de nombre del nombre (serie de caracteres) de entidad (recurso) AppleTalk en una dirección IP AppleTalk (número de 16 bits) en la capa de transporte.

NetBIOS. Network Basic Input/Output System. Interfaz estándar para redes, IBM PC (Personal Computer) y PC compatibles que se utiliza en las LAN para proporcionar funciones de mensajes, de servidor de impresión y de servidor de archivos. Los programas de aplicación que utilizan NetBIOS no necesitan manejar los detalles de protocolos de control de enlace de datos (DLC) de LAN.

nivel de enlace. (1) Parte de la recomendación X.25 que define el protocolo de enlace utilizado para entrar datos en la red y sacarlos de la misma a través del

enlace dúplex que conecta la máquina del abonado con el nodo de red. LAP y LAPB son los protocolos de acceso de enlace recomendados por la CCITT.

(2) Véase *nivel de enlace de datos*.

nivel de enlace de datos. (1) En la estructura jerárquica de una estación de datos, nivel conceptual de control o lógica de proceso entre la lógica de alto nivel y el enlace de datos que mantiene el control del enlace de datos. El nivel de enlace de datos realiza funciones tales como la inserción de bits de transmisión y supresión de bits de recepción; interpretación de campos de dirección y control; generación, transmisión e interpretación de mandatos y respuestas; y cálculo e interpretación de secuencias de comprobación de trama. Véase también *nivel de paquete* y *nivel físico*. (2) En comunicaciones de X.25, sinónimo de *nivel de trama*.

nivel de trama. Sinónimo con *nivel de enlace de datos*. Véase *nivel de enlace*.

nodo. (1) En una red, punto donde una o más unidades funcionales conectan canales o circuitos de datos. (I) (2) Cualquier dispositivo conectado a una red que transmite y recibe datos.

nodo Advanced Peer-to-Peer Networking (APPN). Nodo de red APPN o nodo final APPN.

nodo de destino. Nodo al que se envían datos o una petición.

nodo de esfera de control (SOC). Nodo que está incluido directamente en la esfera de control de un punto focal. Un nodo de SOC ha intercambiado elementos de habilitación de los servicios de gestión con su punto focal. Un nodo final APPN puede ser un nodo de SOC si da soporte a la función de intercambio de elementos de habilitación de los servicios de gestión.

nodo de red (NN). Véase *nodo de red Advanced Peer-to-Peer Networking (APPN)*.

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 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 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 intermedio. Nodo que está al final de más de una rama. (T)

nodos adyacentes. Dos nodos conectados conjuntamente por una vía de acceso, como mínimo, que no conecta ningún otro nodo. (T)

nombre de comunidad. En el protocolo Simple Network Management Protocol (SNMP), serie de octetos que identifica a una comunidad.

nombre de dominio. En el conjunto de protocolos de Internet, nombre de un sistema principal. Un nombre de dominio está compuesto por una secuencia de subnombres separados por un carácter delimitador. Por ejemplo, si el nombre de dominio calificado al completo (FQDN) de un sistema principal es `ra1vm7.vnet.ibm.com`, cada uno de los siguientes es un nombre de dominio:

- `ra1vm7.vnet.ibm.com`
- `vnet.ibm.com`
- `ibm.com`

notación de sintaxis de abstracción 1 (ASN.1). Método de Interconexión de Sistemas Abiertos (OSI) para la sintaxis de abstracción que se especifica en las normas siguientes:

- ITU-T recomendación X.208 (1988) | ISO/IEC 8824: 1990
- ITU-T recomendación X.680 (1994) | ISO/IEC 8824-1: 1994

Véase también *normas básicas de codificación (BER)*.

notación 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.

número de LP. Número de partición lógica. Permite que diversas particiones lógicas de sistema principal, LP, compartan una sola fibra de ESCON. Este valor está definido en el programa de configuración de la entrada/salida (IOCP) del sistema principal mediante la instrucción de macro RESOURCE. Si el sistema principal no utiliza EMIF, utilice el valor por omisión de 0 para el número de LP.

número de puerto. En comunicaciones de Internet, identificación de una entidad de aplicación para el servicio de transporte.

número de secuencia. En comunicaciones, número asignado a una trama o paquete determinados 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 distinguan los sistemas autónomos.

Nways Switch. Sinónimo con IBM 2220 Nways BroadBand Switch.

O

objeto de la MIB. Sinónimo de *variable de la MIB*.

Open Shortest Path First (OSPF). En el conjunto de protocolos de Internet, función que proporciona transferencia de información intradominio. Como alternativa al protocolo Routing Information Protocol (RIP), OSPF permite el direccionamiento de menor coste y lo maneja en grandes redes regionales o corporativas.

Organización Internacional para la Normalización (ISO). Organización de corporaciones nacionales de normas de varios países establecida para promocionar el desarrollo de normas con el fin de facilitar el intercambio internacional de artículos y servicios además de desarrollar la cooperación en la actividad intelectual, científica, tecnológica y económica.

origen. Unidad lógica (LU) externa o programa de aplicación de donde parten un mensaje u otros datos. Véase también *destino*.

P

paquete. En la comunicación de datos, secuencia de dígitos binarios, con inclusión de señales de control y datos, que se transmite y se conmuta como un todo compuesto. Los datos, las señales de control y, posiblemente, la información de control de errores se ordenan siguiendo un formato específico. (I)

paquete de datos. En comunicaciones de X.25, paquete utilizado para la transmisión de datos de usuario dentro de un circuito virtual en la interfaz DTE/DCE.

paquete de petición de llamada. (1) Paquete de supervisión de llamada que un equipo terminal de datos (DTE) transmite con el fin de solicitar que se establezca una conexión para una llamada en la red. (2) En comunicaciones de X.25, paquete de supervisión de llamada transmitido por un DTE para solicitar el establecimiento de una llamada en la red.

paquete de petición de restablecimiento. En comunicaciones X.25, paquete transmitido por el equipo terminal de datos (DTE) al equipo de terminación de circuito de datos (DCE) para solicitar que se restablezca una llamada virtual o un circuito virtual permanente. En el paquete también puede especificarse la razón de la petición.

paquete de recepción no preparada (RNR). Véase *paquete de RNR*.

paquete de RNR. Paquete utilizado por un equipo terminal de datos (DTE) o por un equipo de terminación de circuito de datos (DCE) con el fin de indicar una incapacidad temporal para aceptar paquetes adicionales de petición de llamada virtual o circuito virtual permanente.

paquete explorador. En las LAN, paquete que está generado por el sistema principal de origen y que atraviesa toda la parte de direccionamiento de origen de una LAN con el fin de recoger información sobre las posibles vías de acceso que se encuentran disponibles para el sistema principal.

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.

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.

partición lógica. Número asignado a una partición de un sistema principal que puede funcionar en modalidad lógicamente particionada (LPAR). En modalidad LPAR, el adaptador de ESCON puede compartir una conexión de fibra física con diversas particiones de sistema principal.

pasarela. (1) Unidad funcional que interconecta dos redes de sistema con arquitecturas de red diferentes. Una pasarela conecta redes o sistemas de arquitecturas diferentes. Un puente interconecta redes o sistemas con la misma arquitectura o con arquitecturas similares. (T) (2) En la Red en Anillo de IBM, dispositivo y software asociado que conectan una red de área local a otra red de área local o sistema principal que utiliza protocolos de enlace lógico diferentes. (3) En TCP/IP, sinónimo de *direccionador*.

pasarela exterior. En comunicaciones de Internet, pasarela de un sistema autónomo que comunica con otro sistema autónomo. Compárese con *pasarela interior*.

pasarela interior. En comunicaciones de Internet, pasarela que sólo comunica con su propio sistema autónomo. Compárese con *pasarela exterior*.

período de duración (TTL). Técnica utilizada por los protocolos de entrega de mayor eficacia para impedir que los paquetes se repitan en bucle de manera interminable. El paquete se elimina si el contador de TTL alcanza el valor de 0.

petionario de LU dependientes (DLUR). Nodo final APPN o nodo de red APPN que posee LU dependientes pero solicita que un servidor de LU dependientes proporcione los servicios del SSCP para estas LU dependientes.

Point-to-Point Protocol (PPP). Protocolo que proporciona un método para encapsular y transmitir paquetes sobre enlaces serie punto a punto.

portadora. Tren de pulsaciones u ondas eléctricas o electromagnéticas que puede variar según una señal con información a transmitir sobre un sistema de comunicaciones. (T)

procesador de componente frontal. Procesador, como, por ejemplo, el IBM 3745 ó el 3174, que releva a un sistema principal de las tareas de control de comunicaciones.

proceso a tiempo real. Manipulación de los datos que un proceso necesita o genera mientras el proceso está en funcionamiento. Normalmente, los resultados se utilizan para influir en el proceso, y quizá en procesos relacionados, mientras se está desarrollando.

proporción de pérdida de un paquete. Probabilidad que tiene un paquete de no alcanzar su destino o de no alcanzarlo dentro del período especificado.

protocolo. (1) Conjunto de normas semánticas y sintácticas que determinan el comportamiento de las unidades funcionales a la hora de conseguir la comunicación. (I) (2) En la arquitectura Interconexión de Sistemas Abiertos, conjunto de normas semánticas y sintácticas que determinan el comportamiento de las entidades de la misma capa a la hora de desempeñar funciones de comunicación. (T) (3) En SNA, significados y normas de puesta en secuencia de las peticiones y respuestas que se utilizan para gestionar la red, transferir datos y sincronizar los estados de los componentes de la red. Sinónimo con *disciplina de control de línea* y *disciplina de línea*. Véase *protocolo delimitador* y *protocolo de enlace*.

protocolo de acceso de enlace equilibrado (LAPB). Protocolo utilizado para acceder a una red X.25 en el nivel de enlace. LAPB es un protocolo simétrico, asíncrono y dúplex que se utiliza en la comunicación punto a punto.

protocolo de control de enlace lógico (LLC). En una red de área local, protocolo que dirige el intercambio de tramas de transmisión entre estaciones de datos independientemente de cómo está compartido el medio de transmisión. (T) El protocolo de LLC se desarrolló en la comisión de IEEE 802 y es común a todas las normas de LAN.

protocolo de control del acceso al medio (MAC). En una red de área local, protocolo que dirige el acceso al medio de transmisión, teniendo en cuenta los aspectos topológicos de la red, con el fin de permitir el intercambio de datos entre estaciones de datos. (T)

protocolo de direccionamiento. Técnica utilizada por un direccionador para encontrar otros direccionadores y mantener información actualizada sobre la mejor manera de acceder a las redes asequibles.

protocolo de interfaz de gestión local (LMI). En un NCP, conjunto de procedimientos y mensajes de gestión de red frame-relay utilizados por nodos frame-relay adyacentes para intercambiar información de estado de línea sobre el DLCI X'00'. Un NCP da soporte tanto a la versión del protocolo de LMI del American National Standards Institute (ANSI) como a la de la Comisión Consultiva de la Telefonía y Telegrafía Internacionales (ITU-T/CCITT). Estas normas se refieren al protocolo de LMI como *pruebas de verificación de integridad de enlace (LIVT)*.

prueba de bucle de retorno. Prueba donde las señales de un comprobador se repiten en bucle en un módem u otro elemento de red hacia el comprobador

para tomar medidas que determinen o verifiquen la calidad de la vía de acceso de comunicaciones.

punteo. Unidad funcional que interconecta diversas LAN (local o remotamente) que utilizan el mismo protocolo de control de enlace lógico pero pueden utilizar diferentes protocolos de control del acceso al medio. Un puente reenvía una trama a otro puente basándose en la dirección del control del acceso al medio (MAC).

punteo de ruta. Función de un programa de puente de IBM que permite que dos sistemas de puente utilicen un enlace de telecomunicaciones para conectar dos LAN. Cada sistema de puente se conecta directamente a una de las LAN y el enlace de telecomunicaciones conecta los dos sistemas de puente.

punteo raíz. Puente que es la raíz de un árbol de expansión formado entre otros puentes activos de la red de funciones de puente. El puente raíz origina y transmite unidades de datos de protocolo de puente (BPDU) a otros puentes activos para mantener la topología de árbol de expansión. Es el puente con la prioridad superior de la red.

puentes paralelo. Par de puentes conectados al mismo segmento de LAN que crean vías de acceso redundantes para el segmento.

puerto. (1) Punto de acceso para la entrada o salida de datos. (2) Conector de un dispositivo al que se conectan cables para otros dispositivos, como, por ejemplo, estaciones de pantalla o impresoras. (3) Representación de una conexión física con el hardware de enlace. A veces, un puerto viene referido como adaptador; no obstante, en un adaptador puede haber más de un puerto. Un solo proceso de DLC puede controlar uno o más puertos. (4) En el conjunto de protocolos de Internet, número de 16 bits utilizado para la comunicación entre TCP o el protocolo User Datagram Protocol (UDP) y una aplicación o protocolo de nivel superior. Algunos protocolos, como, por ejemplo, File Transfer Protocol (FTP) y Simple Mail Transfer Protocol (SMTP), utilizan el mismo número de puerto conocido en todas las implementaciones de TCP/IP. (5) Abstracción utilizada por protocolos de transporte para establecer diferencias entre los diversos destinos en una máquina de sistema principal. (6) Sinónimo con *socket*.

puerto de destino. Adaptador asíncrono de 8 puertos que sirve de punto de conexión con un servicio serie.

punto de acceso a servicios (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 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 control (CP). (1) Componente de un nodo APPN o LEN que gestiona los recursos de dicho nodo. En un nodo APPN, el CP puede dedicarse a establecer sesiones de CP-CP con otros nodos APPN. En un nodo de red APPN, el CP también proporciona servicios a nodos finales adyacentes de la red APPN. (2) Componente de un nodo que gestiona los recursos de dicho nodo y, opcionalmente, proporciona servicios a otros nodos de la red. Pueden citarse como ejemplos el punto de control de servicios del sistema (SSCP) de un nodo de subárea de tipo 5, el punto de control de nodo de red (NNCP) de un nodo de red APPN y el punto de control de nodo final (ENCP) de un nodo final APPN o LEN. Un SSCP y un NNCP pueden proporcionar servicios a otros nodos.

punto de control de servicios del sistema (SSCP). Componente de una red de subárea destinado a gestionar la configuración, coordinar las peticiones del operador de red y las de determinación de problemas y proporcionar servicios de directorios además de otros servicios de sesiones para los usuarios de la red. Diversos SSCP, cooperando como iguales entre sí, pueden dividir la red en dominios de control y tener, cada uno de los SSCP, una relación de control jerárquica con las unidades físicas y las unidades lógicas de su propio dominio.

punto de entrada (EP). En SNA, nodo de tipo 2.0, tipo 2.1, tipo 4 ó tipo 5 que proporciona soporte de gestión de redes distribuidas. Envía datos de gestión de redes sobre sí mismo y los recursos que controla a un punto focal para el proceso centralizado, y recibe y ejecuta los mandatos iniciados por el punto focal para gestionar y controlar sus recursos.

R

rastreo. (1) Registro de la ejecución de un programa de sistema. Muestra las secuencias en que se han ejecutado las instrucciones. (A) (2) Para los enlaces de datos, registro de las tramas y bytes transmitidos o recibidos.

recepción no preparada (RNR). En comunicaciones, mandato o respuesta de enlace de datos que indica una condición temporal de incapacidad para aceptar tramas de entrada.

reconfiguración dinámica (DR). Proceso consistente en cambiar la configuración de una red (las PU y LU periféricas) sin regenerar las tablas de configuración al completo ni desactivar el nodo principal afectado.

recurso. En Nways Switch, elemento de hardware o entidad lógica creados por Control Program. Por ejemplo, los adaptadores, LIC y líneas son recursos físicos. Los puntos de control y conexiones son recursos lógicos.

red. (1) Configuración de software y dispositivos de proceso de datos conectados para el intercambio de información. (2) Grupo de nodos y los enlaces que los interconectan.

red Advanced Peer-to-Peer Networking (APPN). Conjunto de nodos de red interconectados y sus nodos finales clientes.

red APPN. Véase *red Advanced Peer-to-Peer Networking (APPN)*.

red de área amplia (WAN). (1) Red que proporciona servicios de comunicación a un área geográfica mayor que la servida por una red de área local o una red de área metropolitana, y que puede utilizar o proporcionar recursos públicos de comunicación. (T) (2) Red de comunicación de datos diseñada para servir a un área de cientos o miles de kilómetros; por ejemplo, las redes públicas y privadas de conmutación de paquetes y las redes telefónicas nacionales. (3) Compárese con *red de área local (LAN)* y *red de área metropolitana (MAN)*.

red de área local (LAN). (1) Red de sistema ubicada en el lugar de un usuario dentro de un área geográfica limitada. La comunicación dentro de una red de área local no está sujeta a reglamentos externos; no obstante, la comunicación más allá del límite de una LAN puede estar sujeta a alguna forma de reglamento. (T) (2) Red en la que un conjunto de dispositivos están conectados entre sí para la comunicación y que puede conectarse a una red mayor. (3) Véase también *Ethernet* y *Red en Anillo*. (4) Compárese con *red de área metropolitana (MAN)* y *red de área amplia (WAN)*.

red de área metropolitana (MAN). Red formada por la interconexión de dos o más redes que puede funcionar a una velocidad mayor que éstas, puede atravesar límites administrativos y puede utilizar diversos métodos de acceso. (T) Compárese con *red de área local (LAN)* y *red de área amplia (WAN)*.

red de clase A. En comunicaciones de Internet, red en la que el bit situado más a la izquierda (más significativo) de la dirección IP está establecido en 0 y el ID 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 ID 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 final a final 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 IEEE 802.5, tecnología de red que controla el acceso al medio pasando una señal (paquete o trama especial) entre las estaciones conectadas al medio. (2) Red FDDI o IEEE 802.5 con una topología de anillo que pasa señales de una estación de anillo de conexión (nodo) a otra. (3) Véase también *red de área local (LAN)*.

red óptica síncrona (SONET). Norma de los EE.UU. para la transmisión de información digital sobre interfaces ópticas. Está estrechamente relacionada con la recomendación sobre la jerarquía digital síncrona (SDH).

red según Red en Anillo. (1) Red de tipo anillo que permite la transmisión de datos unidireccional entre estaciones de datos, mediante un procedimiento consistente en pasar señales, de tal manera que los datos transmitidos vuelven a la estación transmisora. (T)

(2) Red que utiliza una topología de anillo, según la cual pasan señales en un circuito de nodo a nodo. Un nodo que está preparado para emitir puede capturar la señal e insertar datos para la transmisión.

red troncal. Red central a la que se conectan redes más pequeñas, casi siempre de menor velocidad. Normalmente, la red troncal tiene una capacidad muy superior a las redes a las que ayuda a interconectarse o es una red de área amplia (WAN), como, por ejemplo, una red pública de datagramas de paquetes conmutados.

reensamblaje. En comunicaciones, proceso consistente en volver a juntar paquetes segmentados después de haberlos recibido.

Registro sin vuelta a cero y con cambios en los unos (NRZ-1). Método de registro donde los unos están representados mediante un cambio en la condición de magnetización y los ceros están representados mediante la ausencia de cambio. Sólo se registran explícitamente las señales de los unos. (Denominado anteriormente registro *sin vuelta a cero invertido*, NRZI.)

Remote Execution Protocol (REXEC). Protocolo que permite la ejecución de un mandato o programa en cualquier sistema principal de la red. El sistema principal local recibe los resultados de la ejecución del mandato.

remoto. (1) Perteneciente a un sistema, programa o dispositivo al que se accede mediante una línea de telecomunicaciones. (2) Sinónimo de *conectado mediante enlace*. (3) Compárese con *local*.

Request for Comments (RFC). En comunicaciones de Internet, serie de documentos que describe una parte del conjunto de protocolos de Internet y experimentos relacionados. Todas las normas de Internet están documentadas como RFC.

resolución de direcciones. (1) Método para correlacionar direcciones de capa de red con direcciones específicas de los medios. (2) Véase también *Address Resolution Protocol (ARP)* y *AppleTalk Address Resolution Protocol (AARP)*.

resolución de nombres. En comunicaciones de Internet, proceso consistente en correlacionar un nombre de máquina con la dirección Internet Protocol (IP) correspondiente. Véase también *Sistema de nombres de dominio (DNS)*.

respuesta a excepción (ER). En SNA, protocolo solicitado en el campo de formato de respuesta solicitado de la cabecera de una petición que indica al receptor que devuelva una respuesta sólo si la petición no es aceptable tal como se recibe o si no puede procesarse;

es decir, puede devolverse una respuesta negativa, pero no una respuesta positiva. Compárese con *respuesta definida y sin respuesta*.

restablecimiento. En un circuito virtual, reinicialización del control del flujo de datos. En el restablecimiento, se eliminan todos los datos en tránsito.

ritmo. (1) Técnica mediante la cual un componente de recepción controla la velocidad de transmisión de un componente de emisión para evitar un desbordamiento o una congestión. (2) Véase también *control del flujo*, *ritmo de recepción*, *ritmo de emisión*, *ritmo de nivel de sesión* y *ritmo de ruta virtual (VR)*.

rlogin (inicio de sesión remoto). Servicio ofrecido por los sistemas de Berkeley basados en UNIX que permite que los usuarios autorizados de una máquina se conecten con otros sistemas UNIX en una internet e interactúen como si sus terminales estuvieran conectados directamente. El software rlogin pasa información sobre el entorno del usuario (por ejemplo, el tipo de terminal) a la máquina remota.

Routing Information Protocol (RIP). En el conjunto de protocolos de Internet, protocolo de pasarela interior utilizado para intercambiar información de direccionamiento intradominio y para determinar las rutas óptimas entre los sistemas principales de internet. RIP determina las rutas óptimas sobre la base de la métrica de ruta y no sobre la base de la velocidad de transmisión de un enlace.

Routing Table Maintenance Protocol (RTMP). En redes AppleTalk, protocolo que proporciona generación y mantenimiento de información de direccionamiento en la capa de transporte por medio de la tabla de direccionamiento AppleTalk. La tabla de direccionamiento AppleTalk dirige la transmisión de paquetes por la internet de socket de origen a socket de destino.

RouTing update Protocol (RTP). Protocolo de Vrtual 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 la 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 la Red en Anillo de IBM, servidor que acepta mandatos del LAN Network Manager (LNM) para obtener información de estaciones, establecer parámetros de estación y eliminar estaciones de su anillo. Este servidor también recoge y reenvía informes de configuración generados por estaciones de su anillo. Los informes de configuración incluyen los nuevos informes del supervisor activo y los informes de estación contigua activa de donde proceden los datos (NAUN).

servidor de nombres. En el conjunto de protocolos de Internet, sinónimo de *servidor de nombres de dominio*.

servidor de nombres de dominio. En el conjunto de protocolos de Internet, programa servidor que sumi-

nistra 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 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 (NAUs) 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 final a final entre un usuario de marcación y los LNS; sin tener en cuenta si el usuario inicia la sesión o si el LNS inicia una llamada hacia fuera. Los datagramas para la sesión se envían por el túnel entre el LAC y el LNS. Los LNS y LAC mantienen la información de estado para cada usuario conectado a un LAC.

Simple Network Management Protocol (SNMP). En el conjunto de protocolos de Internet, protocolo de gestión de red que se utiliza para supervisar direccionadores y redes conectadas. SNMP es un protocolo de capa de aplicación. La información sobre los dispositivos gestionados está definida y almacenada en la Base de la información de gestión (MIB) de la aplicación.

simulación. Para los enlaces de datos, técnica mediante la cual un protocolo iniciado en una estación final se reconoce con acuse de recibo y se procesa en un nodo intermedio en nombre del destino final. En la conmutación del enlace de datos del IBM 6611, por ejemplo, las tramas de SNA se encapsulan en paquetes de TCP/IP para el transporte a través de una

red de área amplia diferente de SNA, se desempaquetan en otro IBM 6611 y pasan al destino final. Una ventaja de la simulación es que se evitan tiempos de espera 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 petición con eco de Internet Control Message Protocol (ICMP) y esperando una respuesta. (2) En comunicaciones, prueba de asequibilidad.

sondeo. (1) En una conexión multipunto o conexión punto a punto, proceso consistente en invitar a las estaciones de datos a transmitir, una por una. (I) (2) Interrogar a dispositivos con el fin de evitar contenciones, determinar el estado operativo o determinar la disposición para enviar o recibir datos. (A)

soporte de diversos dominios (MDS). Técnica para transportar datos de servicios de gestión entre conjuntos de funciones de servicios de gestión sobre sesiones de LU-LU y CP-CP. Véase también *unidad de mensajería 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 direccionables 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 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 ID 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. (1) (2) Intervalo de tiempo asignado para que tengan lugar determinadas operaciones; por ejemplo, la respuesta a un sondeo o direccionamiento antes de que se interrumpa el funcionamiento del sistema y deba reiniciarse.

topología. En comunicaciones, ordenación física o lógica de los nodos de una red, especialmente las relaciones de un nodo con otro nodo y los enlaces entre los mismos.

trama. (1) En la arquitectura Interconexión de Sistemas Abiertos, estructura de datos perteneciente a un área particular de información y compuesta por ranuras que pueden aceptar los valores de atributos específicos y de las que pueden deducirse inferencias mediante conexiones apropiadas de procedimiento. (T) (2) Unidad de transmisión en algunas redes de área

local, incluida la Red en Anillo de IBM. Incluye delimitadores, caracteres de control, información y caracteres de comprobación. (3) En SDLC, vehículo para cada mandato, cada respuesta y toda información transmitida con procedimientos de SDLC.

trama de información (I). Trama de formato I que se utiliza para la transferencia de información numerada.

trama exploradora. Véase *paquete explorador*.

trama I. Trama de información.

transceptor (transmisor-receptor). En las LAN, dispositivo físico que conecta una interfaz de sistema principal a una red de área local, como, por ejemplo, Ethernet. Los transceptores de Ethernet contienen elementos electrónicos que aplican señales al cable y que detectan colisiones.

Transmission Control Protocol (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.

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.

transporte de vector de gestión de red (NMVT). Unidad de petición/respuesta (RU) de servicios de gestión que fluye sobre una sesión activa entre servicios de gestión de unidad física y servicios de gestión de punto de control (sesión de SSCP-PU).

troncal. (1) En una configuración de anillo de diversos puentes de una red de área local, enlace de gran velocidad al que se conectan los anillos por medio de puentes o direccionadores. Un troncal puede configurarse como bus o como anillo. (2) En una red de área amplia, enlace de gran velocidad al que se conectan nodos o intercambios de conmutaciones de datos (DSE).

Túnel. Un túnel está definido mediante un par LNS-LAC. El túnel lleva datagramas de PPP entre el LAC y el LNS. Un solo túnel puede multiplexar muchas sesiones. Una conexión de control que funciona sobre el mismo túnel controla el establecimiento, liberación y mantenimiento de todas las sesiones y del túnel en sí.

U

umbral. (1) En programas de puente de IBM, valor asignado al número máximo de tramas que no se reen-vían 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 (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 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 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 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, mayor unidad de datos posible que puede enviarse por un medio físico determinado en una sola trama. Por ejemplo, la MTU para Ethernet tiene 1500 bytes.

Unión de Telecomunicaciones Internacionales (ITU). Agencia de telecomunicaciones especializada de las Naciones Unidas que se ha establecido con el fin de proporcionar procedimientos y prácticas para la normalización de las comunicaciones, lo cual incluye asignación de frecuencia y regulaciones de la radio universales.

User Datagram Protocol (UDP). En el conjunto de protocolos de Internet, protocolo que proporciona un

servicio no fiable de datagramas sin conexiones. Permite que un programa de aplicación de una máquina o proceso envíe un datagrama a un programa de aplicación de otra máquina o proceso. UDP utiliza Internet Protocol (IP) para entregar datagramas.

V

V.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.

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.

vertimiento 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.

vía de acceso. (1) En una red, cualquier ruta entre dos nodos cualesquiera. Una vía de acceso puede incluir más de una rama. (T) (2) Serie de componentes de red de transporte (control de la vía de acceso y control de enlace de datos) por los que pasa la información intercambiada entre dos unidades de red accesibles. Véase también *ruta explícita (ER)*, *extensión de ruta* y *ruta virtual (VR)*.

VINES. Virtual NETworking System.

Virtual Networking System (VINES). Sistema operativo de red y software de red de Banyan Systems, Inc. En una red VINES, la función de enlace virtual permite que todos los dispositivos y servicios aparenten estar conectados directamente entre sí cuando en realidad pueden encontrarse a miles de kilómetros de distancia. Véase también *StreetTalk*.

vista de la MIB. En el protocolo Simple Network Management Protocol (SNMP), conjunto de objetos gestionados, conocidos por el agente, que es visible en una comunidad en particular.

vuelco. (1) Datos que se han volcado. (T)
(2) Copiar el contenido de la totalidad o de parte del almacenamiento virtual con el fin de reunir información de errores.

X

X.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.

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*.

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

- AAA, atributos remotos 613
- accept-qos-parms-from-lecs
 - QoS 291
- acceso a la Antememoria de Host On-Demand Client 159
- acceso a la Antememoria del servidor de la web 214
- acceso al indicador de configuración de autenticación 259
- ACE/Server
 - autenticación 256
- activate
 - mandato de configuración de Antememoria de Host On-Demand Client 160
 - mandato de configuración de la Antememoria del servidor de la web 214
 - mandato de supervisión de Antememoria de Host On-Demand Client 164
 - mandato de supervisión de la Antememoria del servidor de la web 222
- activate-ip-precedence-filtering
 - mandato de configuración de reserva de ancho de banda 31
- add
 - mandato de actualización de filtrado MAC 64
 - mandato de configuración de Antememoria de Host On-Demand Client 160
 - mandato de configuración de la Antememoria del servidor de la web 215
 - mandato de configuración de Restauración de WAN 78
 - mandato de configuración de TSF 592
 - mandatos de configuración de servidor DHCP 540
- add server
 - mandato de configuración de seguridad de IP 389
- add tunnel
 - mandato de configuración de seguridad de IP 394
- add-circuit-class
 - mandato de configuración de reserva de ancho de banda 31
- add-class
 - mandato de configuración de reserva de ancho de banda 31
- AH 370
- algoritmos para seguridad de IP (IPv4) 392
- algoritmos para seguridad de IP (IPv6) 405
- Antememoria de Host On-Demand Client
 - configuración y supervisión 155
 - definición de un cluster 121
- Antememoria escalable de alta disponibilidad 176

- asociación de seguridad (SA) 372
- assign
 - mandato de configuración de reserva de ancho de banda 33
- assign-circuit
 - mandato de configuración de reserva de ancho de banda 37
- atributos AAA remotos 613
 - palabras clave 613
 - radius 613
 - TACACS 614
- attach
 - mandato de configuración de filtrado MAC 60
- autenticación 251, 259
 - mandatos de configuración 259
 - seguridad 251
 - utilización de SecurID 256
 - limitaciones 257
- autenticación del Gestor de control de antememoria externa 180
- autorización
 - seguridad 251

C

- cabecera de autenticación (AH) 370
- Calidad de los servicios 285
 - Véase también* QoS
- características
 - Calidad de los servicios (QoS) 285
 - Característica Thin Server (TSF) 577
 - filtrado MAC 55, 59
 - reserva de ancho de banda 1
 - supervisión 25
- características de puente
 - filtrado MAC 59
 - mandatos de actualización 64
 - submandatos de actualización 57
- carga de seguridad de encapsulación (ESP) 371
- cert-load
 - mandato de supervisión de PKI (IPv4) 413
- cert-req
 - mandato de supervisión de PKI (IPv4) 414
- cert-save
 - mandato de supervisión de PKI (IPv4) 414
- certificado
 - obtención 388
- cifrado
 - configuración 279
 - para frame relay 282
 - configuración de ECP
 - para PPP 280

- cifrado (*continuación*)
 - configuración de MPPE
 - para PPP 281
 - frame relay 279
 - PPP 279
 - supervisión
 - para frame relay 283
 - para PPP 280
 - supervisión de MPPE
 - para PPP 282
- cifrado ECP
 - configuración
 - para PPP 280
- Cifrado punto a punto MS
 - configuración 279
 - para PPP 281
- circuit
 - mandato de configuración de reserva de ancho de banda 37
 - mandato de supervisión de Reserva de ancho de banda 52
- circuito de marcación
 - valores por omisión de parámetros
 - para interfaces de marcación de entrada 488
- claves 387
 - para seguridad de IP (IPv4), configuración 393
 - para seguridad de IP (IPv6), configuración 405
- claves de cifrado 387
 - para seguridad de IP (IPv4), configuración 393
- clear
 - mandato de supervisión de Antememoria de Host On-Demand Client 165
 - mandato de supervisión de filtrado MAC 68
 - mandato de supervisión de la Antememoria del servidor de la web 223
 - mandato de supervisión de Reserva de ancho de banda 52
 - mandato de supervisión de VCRM 610
 - mandatos de supervisión de Restauración de WAN 86
- clear-block
 - mandato de configuración de reserva de ancho de banda 38
- clear-circuit-class
 - mandato de supervisión de Reserva de ancho de banda 52
- códigos de retorno 204
 - código de retorno y descripciones 204
- colocación en antememoria 171
- compresión
 - visión general
 - frame relay 237
 - PPP 237
- compresión de datos
 - conceptos 237
 - conceptos básicos 238
- compresión de datos (*continuación*)
 - consideraciones 240
 - carga de la CPU 241
 - compresión de capa de enlaces 242
 - contenido de datos 242
 - utilización de la memoria 241
 - diccionario de datos
 - definición de 238
 - en enlaces Frame Relay 245
 - configuración 245
 - supervisión 247
 - historial
 - definición de 239
 - sesiones de compresión
 - definición de 241
 - visión general 237
- configuración 387
 - acceso al indicador de autenticación 259
 - cifrado 279
 - para frame relay 282
 - cifrado ECP
 - para PPP 280
 - Cifrado punto a punto MS 279
 - compresión de datos en enlaces Frame Relay 245
 - compresión de datos en enlaces PPP 243
 - diffserv 431
 - Infraestructura de clave pública 388
 - Intercambio de claves de Internet 387
 - interfaz de marcación de entrada 488
 - LDAP 343
 - MPPE
 - para PPP 281
 - políticas 343
 - protocolos L2 453
 - Restauración de WAN 77
 - seguridad de IP (IPv6) 404
 - seguridad de IP manual (IPv4) 392
 - túnel manual (IPv4) 402
 - túnel manual (IPv6) 406
- configuración y supervisión de la Antememoria del servidor de la web 207
- consejeros
 - para network dispatcher 108
- contabilidad
 - seguridad 251
- Conversión de direcciones de red
 - configuración 477
 - mandatos de supervisión de la 484
- Conversión de direcciones de red (NAT)
 - Véase también ?*
 - utilización de 469
- Conversión de puertos de direcciones de red (NAPT)
 - utilización de 470
- correlaciones de direcciones estáticas 471
- counters
 - mandato de supervisión de Reserva de ancho de banda 52

- counters-circuit-class
 - mandato de supervisión de Reserva de ancho de banda 53
- create
 - mandatos de configuración de filtrado MAC 60
- create-super-class
 - mandato de configuración de reserva de ancho de banda 39

CH

- change
 - mandato de Conversión de direcciones de red 478
 - mandato de NAT 478
 - mandatos de configuración de servidor DHCP 546
- change server
 - mandato de configuración de seguridad de IP 389
- change tunnel
 - mandato de configuración de seguridad de IP 399
 - mandato de supervisión de seguridad de IP 417
- change-circuit-class
 - mandato de configuración de reserva de ancho de banda 37
- change-class
 - mandato de configuración de reserva de ancho de banda 37

D

- deactivate-ip-precedence-filtering
 - mandato de configuración de reserva de ancho de banda 39
- deassign
 - mandato de configuración de reserva de ancho de banda 39
- deassign-circuit
 - mandato de configuración de reserva de ancho de banda 39
- default
 - mandato de configuración de filtrado MAC 61
- default-circuit-class
 - mandato de configuración de reserva de ancho de banda 40
- default-class
 - mandato de configuración de reserva de ancho de banda 40
- definición de un cluster
 - Antememoria de Host On-Demand Client 121
- del-circuit-class
 - mandato de configuración de reserva de ancho de banda 40
- del-class
 - mandato de configuración de reserva de ancho de banda 40
- delete
 - mandato de actualización de filtrado MAC 65

- delete (*continuación*)
 - mandato de configuración de Antememoria de Host On-Demand Client 161
 - mandato de configuración de filtrado MAC 61
 - mandato de configuración de la Antememoria del servidor de la web 215
 - mandato de configuración de TSF 597
 - mandato de Conversión de direcciones de red 478
 - mandato de NAT 478
 - mandato de supervisión de Antememoria de Host On-Demand Client 165
 - mandato de supervisión de la Antememoria del servidor de la web 223
 - mandato de supervisión de seguridad de IP 411
 - mandatos de configuración de servidor DHCP 551
- delete certificate
 - mandato de configuración de seguridad de IP 390
- delete private-key
 - mandato de configuración de seguridad de IP 390
- delete server
 - mandato de configuración de seguridad de IP 390
- delete tunnel
 - mandato de configuración de seguridad de IP (IPv4) 399
 - mandato de supervisión de seguridad de IP 417
- delete-file
 - mandato de supervisión de TSF 601
- descubrimiento de MTU de vía de acceso 375
- detach
 - mandato de configuración de filtrado MAC 62
- DHCP (dynamic host configuration protocol)
 - configuración básica 492
 - descripción 492
 - múltiples saltos a servidor 493
 - red de varios servidores 493
- diagrama de red
 - túnel de seguridad de IP 376
- DIAL
 - definición 487
- DHCP (dynamic host configuration protocol)
 - configuración básica 492
 - descripción 492
 - múltiples saltos a servidor 493
 - red de varios servidores 493
- interfaz de marcación de entrada
 - configuración 488
- mandatos de configuración 490
- mandatos de configuración global 495
- mandatos de supervisión global 503
- requisitos 488
- servidor de nombres de dominio dinámico (DDNS)
 - descripción 494
 - utilización de 487
- dial-in access server
 - direcciones IP proporcionadas por el servidor 490
 - métodos de asignación de direcciones IP 491

diffserv

- característica, resumen 425
- configuración 428, 431
- indicador de configuración
 - acceso 431
- mandatos de configuración
 - delete 432
 - disable 432
 - enable 432
 - list 433
 - resumen 431
 - set 434
- mandatos de supervisión 437
 - clear 437
 - dscache 437
 - list 438
- solicitud de supervisión
 - acceso 436
- terminología 428
- visión general 425

disable

- mandato de configuración de filtrado MAC 62
- mandato de configuración de reserva de ancho de banda 41
- mandato de configuración de Restauración de WAN 79, 87
- mandato de configuración de seguridad de IP 399
- mandato de Conversión de direcciones de red 479
- mandato de NAT 479
- mandato de supervisión de Antememoria de Host On-Demand Client 166
- mandato de supervisión de filtrado MAC 68
- mandato de supervisión de la Antememoria del servidor de la web 224
- mandato de supervisión de seguridad de IP 418
- mandatos de configuración de servidor DHCP 555
- mandatos de supervisión de servidor DHCP 573

disable-hpr-over-ip-port-numbers

- mandato de configuración de reserva de ancho de banda 41

DLSw

- filtrado MAC 55

E

ejecutor

- para network dispatcher 108

enable

- mandato de configuración de filtrado MAC 62
- mandato de configuración de la Conversión de direcciones de red 479
- mandato de configuración de NAT 479
- mandato de configuración de reserva de ancho de banda 41
- mandato de configuración de Restauración de WAN 80

enable (*continuación*)

- mandato de configuración de seguridad de IP 400
- mandato de supervisión de Antememoria de Host On-Demand Client 165
- mandato de supervisión de filtrado MAC 69
- mandato de supervisión de la Antememoria del servidor de la web 223
- mandato de supervisión de Restauración de WAN 88
- mandato de supervisión de seguridad de IP 418
- mandatos de configuración de servidor DHCP 555
- mandatos de supervisión de servidor DHCP 573
- enable-hpr-over-ip-port-numbers
 - mandato de configuración de reserva de ancho de banda 42
- encapsulador PPP
 - valores por omisión de parámetros
 - para interfaces de marcación de entrada 489
- enlaces Frame Relay
 - configuración y supervisión de compresión de datos 245
- enlaces PPP
 - configuración y supervisión de compresión de datos 243
- entorno de supervisión de VCRM
 - acceso 609
- entradas de descriptor de parámetro
 - QoS 304
- equilibrio de carga
 - con network dispatcher 108
- ES
 - configuración 229
 - supervisión 229
- ESP 371
- estadísticas
 - QoS 303

F

filtrado

- direccionamiento de multidifusión 8
- direccionamiento MAC 8
- orden de precedencia 12
- y reserva de ancho de banda 7

filtrado MAC

- acceso al indicador de configuración 59
- acceso al indicador de supervisión 67
- análisis 55
- configuración 59
- para tráfico DLSw 55
- parámetros 56
- submandatos de actualización 57
- utilización de códigos 57

filtros de paquetes para NAT 472

flush

- mandato de supervisión de TSF 602

- formato de subcampo
 - subcampo dependency 202
 - subcampo name 203
 - subcampo object 203
 - subcampo password request 203
 - subcampo URL request 203
- formato de subvector 187
 - subvector de mandato policy 191
 - subvector de mandato purge 194
 - subvector de mandato query 194
 - subvector de mandato statistics 194
 - subvector de mandato URL mask 194
 - subvector de respuesta a add (force) 195
 - subvector de respuesta a add object 195
 - subvector de respuesta a delete object 196
 - subvector de respuesta a dependency 196
 - subvector de respuesta a disable 196
 - subvector de respuesta a enable 197
 - subvector de respuesta a policy 197
 - subvector de respuesta a purge 199
 - subvector de respuesta a query 199
 - subvector de respuesta a URL mask 201
- formatos de subcampo 202
- formatos de subvector
 - subvector de mandato add (force) object 189
 - subvector de mandato add object 188
 - subvector de mandato delete object 189
 - subvector de mandato dependency 189
 - subvector de mandato disable 190
 - subvector de mandato enable 191
- Formatos de vector del Protocolo de control de antememoria externa (ECCP) 183
 - descripciones de campo 184
 - formatos de subvector 187
 - vector de petición de autenticación 185
 - vector de petición de mandato 185
 - vector de respuesta de autenticación 186
 - vector de respuesta de mandato 186
- Frame Relay
 - cifrado 279
 - configuración 282
 - supervisión 283
 - Reserva de ancho de banda 3
- Función de colocación en antememoria del servidor de la web
 - definición de un cluster 121
- función thin server
 - configuración 591

G

- gestor
 - para network dispatcher 109
- Gestor de control de antememoria externa
 - adición de un objeto 181
 - consulta de un objeto 183

- Gestor de control de antememoria externa (*continuación*)
 - depuración de la partición 183
 - descripciones 181
 - inhabilitación/habilitación de una partición 182
 - supresión de un objeto 182
 - utilización de estadísticas 183
 - utilización de la tabla de dependencias 182
 - utilización de políticas 182
 - utilización de una máscara de URL 183
- Gestor de recursos de circuito virtual (VCRM)
 - configuración y supervisión 609

I

- indicador de configuración de autenticación
 - acceso 259
- Infraestructura de clave pública 380
 - acceso al entorno (IPv4) 413
 - configuración 380, 388
 - configuración de la Infraestructura de clave pública 380
 - mandatos de configuración 389
 - add server 389
 - change server 389
 - delete certificate 390
 - delete private-key 390
 - delete server 390
 - list certificates 391
 - list private-keys 391
 - list servers 391
 - mandatos de supervisión 413
 - acceso (IPv4) 413
 - cert-load (IPv4) 413
 - cert-req (IPv4) 414
 - cert-save (IPv4) 414
 - list certificate (IPv4) 414
 - list configured-servers (IPv4) 415
 - load certificate (IPv4) 415
- Intercambio de claves de Internet 377
 - configuración 387
 - configuración de la Infraestructura de clave pública 380
 - fases del intercambio de claves 378
 - intercambios de mensajes 379
 - mandatos de supervisión
 - acceso (IPv4) 410
 - mandatos de supervisión (IPv4) 411
- interface
 - mandato de configuración de reserva de ancho de banda 43
 - mandato de supervisión de Reserva de ancho de banda 54
- interfaces de marcación de entrada
 - valores por omisión de parámetros de circuito de marcación 488

interfaces de marcación de entrada (*continuación*)
valores por omisión de parámetros de encapsulador PPP 489

interfaz de marcación de entrada
adición 489
configuración 488

L

L2F

configuración 453

L2T 443

características soportadas 444

configuración 447

consideraciones

LCP 446

tiempo 446

mandatos de configuración

add 456

disable 454, 456

enable 454, 457

encapsulador 454, 458

list 454, 458

resumen 453, 455

set 454, 459

terminología 443

visión general 443

L2TP

configuración 453

mandatos de supervisión 461

call 461

kill 464

memory 464

start 465

stop 465

tunnel 465

last

mandato de supervisión de Reserva de ancho de banda 54

last-circuit-class

mandato de supervisión de Reserva de ancho de banda 54

LDAP

configuración 343

mandatos de configuración

disable 359

enable 359

resumen 358

set 361

set default-policy 359

set refresh 362

LE-Client

mandato de supervisión de QoS 300

list

mandato de actualización de filtrado MAC 66

mandato de configuración de Antememoria de Host On-Demand Client 161

list (*continuación*)

mandato de configuración de filtrado MAC 62

mandato de configuración de la Antememoria del servidor de la web 216

mandato de configuración de la Conversión de direcciones de red 479

mandato de configuración de NAT 479

mandato de configuración de reserva de ancho de banda 44

mandato de configuración de Restauración de WAN 81

mandato de configuración de seguridad de IP 401

mandato de configuración de TSF 598

mandato de supervisión de Antememoria de Host On-Demand Client 166

mandato de supervisión de Conversión de direcciones de red 485

mandato de supervisión de filtrado MAC 69

mandato de supervisión de la Antememoria del servidor de la web 224

mandato de supervisión de NAT 485

mandato de supervisión de Restauración de WAN 92

mandato de supervisión de seguridad de IP 411, 419

mandato de supervisión de TSF 602

mandatos de configuración de QoS de LE Client 293

mandatos de configuración de servidor DHCP 556, 573

parámetros del subsistema de codificación (talk 5) 232

parámetros del subsistema de codificación (talk 6) 230

list certificate

mandato de supervisión de PKI (IPv4) 414

list certificates

mandato de configuración de seguridad de IP 391

list configured-servers

mandato de supervisión de PKI (IPv4) 415

list private-keys

mandato de configuración de seguridad de IP 391

list servers

mandato de configuración de seguridad de IP 391

load certificate

mandato de supervisión de PKI (IPv4) 415

M

mandato de supervisión de VCRM

clear 610

queue 610

mandato dials 495

mandato feature 591

mandatos

DIAL

configuración global 495

- mandatos (*continuación*)
 - DIAL (*continuación*)
 - supervisión global 503
- mandatos de configuración 387
 - autenticación 259
 - default-policy
 - set 359
 - DIAL 490
 - DIAL global 495
 - diffserv 431
 - delete 432
 - disable 432
 - enable 432
 - list 433
 - set 434
 - IPSec 387
 - acceso (IPv4) 393
 - acceso (IPv6) 405
 - add server 389
 - add tunnel 394
 - change server 389
 - change tunnel 399
 - delete certificate 390
 - delete private-key 390
 - delete server 390
 - delete tunnel (IPv4) 399
 - disable 399
 - enable 400
 - list 401
 - list certificates 391
 - list private-keys 391
 - list servers 391
 - set 402
 - L2 tunneling
 - set 454, 459
 - L2F, resumen de 453, 455
 - L2T
 - add 456
 - disable 454, 456
 - enable 454, 457
 - L2TP
 - call 461
 - encapsulator 454, 458
 - kill 464
 - list 454, 458
 - memory 464
 - start 465
 - stop 465
 - tunnel 465
 - L2TP, resumen de 453, 455
 - LDAP 358
 - disable 359
 - enable 359
 - set 361
 - política 343
 - add 344
 - copy 357
- mandatos de configuración (*continuación*)
 - política (*continuación*)
 - change 357
 - delete 357
 - disable 358
 - enable 358
 - list 358
 - PPTP, resumen de 453, 455
 - refresh
 - set 362
 - túnel
 - add 456
- mandatos de configuración de Antememoria de Host
 - On-Demand Client
 - activate 160
 - add 160
 - delete 161
 - list 161
 - modify 162
- mandatos de configuración de filtrado MAC
 - acceso 59
 - attach 60
 - create 60
 - default 61
 - delete 61
 - detach 62
 - disable 62
 - enable 62
 - list 62
- mandatos de actualización
 - add 64
 - delete 65
 - list 66
 - move 67
 - resumen 64
 - set-action 67
 - move 63
 - reinit 63
 - resumen 59
 - set-cache 63
 - submandatos de actualización 57
 - update 63
- mandatos de configuración de la Antememoria del ser-
 - vidor de la web
 - activate 214
 - add 215
 - delete 215
 - list 216
 - modify 217
- mandatos de configuración de la Conversión de direc-
 - ciones de red 477
 - list 479
- mandatos de configuración de NAT 477
- mandatos de configuración de Redireccionamiento de
 - WAN
 - set 83, 89

mandatos de configuración de Reserva de ancho de banda

- acceso al indicador de configuración de BRS 25
- activate-ip-precedence-filtering 31
- add-circuit-class 31
- add-class 31
- assign 33
- assign-circuit 37
- circuit 37
- clear-block 38
- configuración de ejemplo 13
- create-super-class 39
- change-circuit-class 37
- change-class 37
- deactivate-ip-precedence-filtering 39
- deassign 39
- deassign-circuit 39
- default-circuit-class 40
- default-class 40
- del-circuit-class 40
- del-class 40
- disable 41
- disable-hpr-over-ip-port-numbers 41
- enable 41
- enable-hpr-over-ip-port-numbers 42
- interface 43
- list 44
- queue-length 47
- resumen 26
- set circuit defaults 48
- show 48
- tag 49
- untag 49
- use circuit defaults 50

mandatos de configuración de Restauración de WAN

- add 78
- disable 79
- enable 80
- list 81
- remove 82
- resumen 77

mandatos de configuración de servidor DHCP

- acceso 539
- add 540
- change 546
- delete 551
- disable 555
- enable 555
- list 556, 573
- set 563

mandatos de configuración de tsf

- add 592
- delete 597
- list 598
- modify 598
- resumen 591

mandatos de configuración de tsf (*continuación*)

- set 599
- mandatos de configuración global
- DIAL 495

mandatos de Conversión de direcciones de red

- change 478
- delete 478
- disable 479
- enable 479
- map 480
- reserve 481
- reset 483
- set 483

Mandatos de la Antememoria del servidor de la web 214

mandatos de modificación de Antememoria de Host On-Demand Client

- modify 168

mandatos de modificación de la Antememoria del ser-

- vidor de la web
- modify 227

mandatos de NAT

- change 478
- delete 478
- disable 479
- enable 479
- list 479
- map 480
- reserve 481
- reset 483
- set 483

mandatos de supervisión

- diffserv
- clear 437
- dscache 437
- list 438
- global de DIAL 503
- IPSec 387
- change tunnel 417
- delete 411
- delete tunnel 417
- disable 418
- enable 418
- IKE, acceso (IPv4) 410
- IPSec, acceso (IPv4) 416
- IPSec, acceso (IPv6) 423
- list 411, 419
- PKI, acceso (IPv4) 413
- reset 421
- set 422
- stats 412, 422

política

- disable 363
- enable 364
- list 365
- reset 364
- search 364

- mandatos de supervisión (*continuación*)
 - política (*continuación*)
 - status 365
 - test 366
 - mandatos de supervisión de Antememoria de Host On-Demand Client
 - activate 164
 - clear 165
 - delete 165
 - disable 166
 - enable 165
 - list 166
 - mandatos de supervisión de DIALS
 - acceso 503
 - mandatos de supervisión de filtrado MAC
 - acceso 67
 - clear 68
 - disable 68
 - enable 69
 - list 69
 - reinit 70
 - resumen 67
 - mandatos de supervisión de la Antememoria del servidor de la web
 - activate 222
 - clear 223
 - delete 223
 - disable 224
 - enable 223
 - list 224
 - mandatos de supervisión de Reserva de ancho de banda
 - acceso al indicador de supervisión 50
 - circuit 52
 - clear 52
 - clear-circuit-class 52
 - counters 52
 - counters-circuit-class 53
 - interface 54
 - last 54
 - last-circuit-class 54
 - resumen 51
 - mandatos de supervisión de Restauración de WAN
 - acceso 86
 - clear 86
 - disable 87
 - enable 88
 - list 92
 - resumen 86
 - mandatos de supervisión de servidor DHCP
 - acceso 572
 - disable 573
 - enable 573
 - request 574
 - reset 574
 - mandatos de supervisión de TSF
 - acceso 601
 - delete-file 601
 - file 602
 - flush 602
 - refresh 606
 - reset 606
 - restart 606
 - resumen de 601
 - set 607
 - mandatos de supervisión global
 - DIAL 503
 - map
 - mandato de configuración de la Conversión de direcciones de red 480
 - mandato de configuración de NAT 480
 - marcación en desbordamiento 71
 - max-burst-size
 - QoS 288
 - max-reserved-bandwidth
 - parámetro de QoS 287
 - modalidad de transporte 372
 - modalidad de túnel 372
 - modify
 - mandato de configuración de Antememoria de Host On-Demand Client 162
 - mandato de configuración de la Antememoria del servidor de la web 217
 - mandato de configuración de TSF 598
 - mandato de modificación de Antememoria de Host On-Demand Client 168
 - mandato de modificación de la Antememoria del servidor de la web 227
 - move
 - mandato de actualización de filtrado MAC 67
 - mandato de configuración de filtrado MAC 63
 - MPPE
 - configuración 279
 - para PPP 281
- ## N
- NAPT
 - utilización de 470
 - NAT
 - configuración 477
 - configuración de ejemplo 472
 - correlaciones de direcciones estáticas 471
 - filtros de paquetes 472
 - mandatos de supervisión de la 484
 - reglas de control de acceso 472
 - utilización de 469
 - negotiate-qos
 - QoS 290
 - network dispatcher 107
 - alta disponibilidad 109

- network dispatcher (*continuación*)
 - aplicaciones de gestión de SNMP 108
 - configuración 111
 - consejeros 108
 - ejecutor 108
 - equilibrio de carga 108
 - gestor 109
 - mandato de configuración 107, 125
 - acceso 125, 145
 - add 126
 - clear 133
 - disable 133
 - enable 134
 - list 135, 145
 - quiesce 147
 - remove 136
 - report 148
 - resumen de 125, 145
 - set 139
 - status 149
 - utilización de 107
 - arquitectura de dos niveles
 - pasos 114
 - visión general 107
- Network Dispatcher con Antememoria del servidor de la web y con entradas en la antememoria 171
- Network Dispatcher con Antememoria del servidor de la web y sin entradas en la antememoria 170
- Network Dispatcher sin Antememoria del servidor de la web 170
- Network Station 577
- NSF
 - utilización de TFTP 581

P

- palabras clave 613
- paquetes L2TP
 - y seguridad de IP 374
- parámetros
 - filtrado MAC 56
- peak-cell-rate
 - QoS 287
- petición de antememoria encontrada 176
- petición reenviada a la antememoria responsable 177
- petición reenviada a la antememoria responsable y no encontrada 178
- petición reenviada al servidor de fondo 178
- política
 - característica, resumen 307
 - configuración 343
 - consultas de IP 309
 - consultas de IPSec 309
 - decisión y aplicación 307
 - decisión y flujo de paquetes 308
 - decisiones de IKE 309

- política (*continuación*)
 - decisiones de RSVP 310
 - ejemplos de configuración 320
 - eliminar todo el tráfico público 334
 - esquema 317
 - generación de reglas 319
 - indicador de configuración
 - acceso 343
 - interacción entre LDAP y la base de datos de políticas 315
 - mandatos de configuración
 - add 344
 - copy 357
 - change 357
 - delete 357
 - disable 358
 - enable 358
 - list 358
 - resumen 343
 - mandatos de supervisión 363
 - disable 363
 - enable 364
 - list 365
 - reset 364
 - search 364
 - status 365
 - test 366
 - motor de búsqueda de política LDAP
 - configuración y habilitación 338
 - objetos 310
 - política de IPSec/ISAKMP con QoS 321
 - política única de IPSec/ISAKMP 331
 - solicitud de supervisión
 - acceso 363
 - visión general 307
- PPTP
 - configuración 453
- preparación para operaciones de seguridad de IP negociadas 387
- Protocolo de control de antememoria externa 181
 - configuración 181
- Protocolo de control de cifrado
 - para PPP 279
- Protocolo punto a punto (PPP)
 - Protocolo de control de cifrado 279
- Protocolos de control de red (NCP)
 - para interfaces PPP
 - Protocolo de control de cifrado 279

Q

- QoS
 - accept-qos-parms-from-lecs 291
 - acceso a los mandatos de supervisión 300
 - acceso al indicador de configuración 291
 - Configuración 285

QoS (*continuación*)

- configuraciones 302
- entradas de descriptor de parámetro 304
- estadísticas 303
- mandatos de configuración 292
- mandatos de configuración de interfaz ATM
 - Remove 297, 299
 - Set 297
- mandatos de configuración de LE Client
 - List 293
 - Remove 296
 - Set 293
- mandatos de configuración de LE Client, resumen 292
- mandatos de supervisión
 - LE-Client 300
- mandatos de supervisión de QoS de LE-Client
 - List 301
- max-burst-size 288
- negotiate-qos 290
- parámetro max-reserved-bandwidth 287
- parámetro peak-cell-rate 287
- parámetro traffic-type 287
- parámetros de configuración 286
- qos-class 289
- resumen de mandatos de supervisión 300
- resumen de mandatos de supervisión de QoS de LE-Client 301
- sustained-cell-rate 288
- tabla VCC LEC 305
- tráfico 304
- utilización de 285
- validate-pcr-of-best-effort-vccs 290
- VCC LEC Data Direct 302
- ventajas 285

qos-class

- QoS 289

queue

- mandato de supervisión de VCRM 610

queue-length

- mandato de configuración de reserva de ancho de banda 47

R

radius 613

Redireccionamiento de WAN

- análisis 99
- asignación del enlace alternativo 104
- configuración 101
- configuración de circuitos de marcación 104
- configuración de ejemplo 102
- configuración de Frame Relay 103
- configuración de RDSI 104
- configuración del enlace alternativo 104
- visión general 71

refresh

- mandato de supervisión de TSF 606

reglas de control de acceso para NAT 472

reinit

- mandato de configuración de filtrado MAC 63
- mandato de supervisión de filtrado MAC 70

remotos, atributos AAA 613

remove

- mandato de configuración de Restauración de WAN 82
- mandatos de configuración de QoS de la interfaz ATM 297, 299
- mandatos de configuración de QoS de LE Client 296

request

- mandatos de supervisión de servidor DHCP 574

requisitos

- para dial-in-access server 488

reserva de ancho de banda

- a través de Frame Relay 3
- acceso a indicadores de configuración 25
- acceso a indicadores de supervisión 50
- con filtros 7
- configuración 1
- mandatos de configuración
 - resumen 28

reserve

- mandato de Conversión de direcciones de red 481
- mandato de NAT 481

reset

- configuración de la Conversión de direcciones de red 486
- mandato de configuración de la Conversión de direcciones de red 483
- mandato de configuración de NAT 483, 486
- mandato de supervisión de seguridad de IP 421
- mandato de supervisión de TSF 606
- mandatos de supervisión de servidor DHCP 574

restart

- mandato de supervisión de TSF 606

Restauración de WAN

- configuración de circuito de marcación secundario 74
- procedimiento de configuración 74
- visión general 71

S

SecurID

- descripción 256
- limitaciones 257

seguridad 180

- autenticación 251
- autorización 251
- contabilidad 251

- seguridad AAA
 - seguridad 251
- seguridad de IP 367
 - algoritmos (IPv6) 405
 - anidado de protocolos 374
 - asociación de seguridad (SA) 372
 - cabecera de autenticación (AH) 370
 - carga de seguridad de encapsulación (ESP) 371
 - certificado
 - obtención 388
 - conceptos 368
 - configuración (IPv6) 404
 - configuración de algoritmos (IPv4) 392
 - configuración de algoritmos (IPv6) 405
 - configuración de claves (IPv6) 405
 - configuración de claves de cifrado (IPv4) 393
 - configuración y supervisión 387
 - descubrimiento de MTU de vía de acceso 375
 - Infraestructura de clave pública 380
 - configuración 388
 - mandatos de configuración 389
 - mandatos de supervisión 413
 - Intercambio de claves de Internet 377, 380
 - configuración 387
 - mandatos de supervisión (IPv4) 411
 - mandatos de configuración
 - acceso (IPv4) 393
 - acceso (IPv6) 405
 - add server 389
 - add tunnel 394
 - change server 389
 - change tunnel 399
 - delete 390
 - delete private-key 390
 - delete server 390
 - delete tunnel 399
 - disable 399
 - enable 400
 - list 401
 - list certificates 391
 - list private-keys 391
 - list servers 391
 - set 402
 - mandatos de supervisión
 - acceso (IPv4) 416
 - acceso (IPv6) 423
 - change tunnel 417
 - delete 411
 - delete tunnel 417
 - disable 418
 - enable 418
 - list 411, 419
 - reset 421
 - set 422
 - stats 412, 422
 - mandatos de supervisión (IPv4) 416
- seguridad de IP (*continuación*)
 - mandatos de supervisión (IPv6) 423
 - manual
 - configuración (IPv4) 392
 - supervisión (IPv4) 423
 - manual (IPv4) 385
 - manual (IPv6) 385
 - modalidad de transporte 372
 - modalidad de túnel 372
 - negociado 377
 - intercambios de mensajes 379
 - preparación para operaciones de seguridad de IP negociadas 387
 - supervisión (IPv4) 410
 - supervisión (IPv6) 423
 - supervisión del Intercambio de claves de Internet (IPv4) 410
 - terminología 368
 - túnel
 - diagrama de red 376
 - túnel en túnel 375
 - túnel manual
 - configuración (IPv4) 402
 - configuración (IPv6) 406
 - túneles seguros 367
 - utilización de 367
 - AH y ESP 372
 - visión general 367
 - y paquetes L2TP 374
- seguridad de IP manual 387
 - IPv4 385
 - IPv6 385
 - mandatos de configuración 393
 - supervisión (IPv6) 423
- seguridad de IP negociada 377
 - fases del intercambio de claves IKE 378
 - intercambios de mensajes 379
 - intercambios de mensajes IKE 379
 - operaciones
 - preparación para 387
- servidor
 - ACE/Server
 - limitaciones 257
 - soporte 256
 - autenticación
 - definición 256
 - DIAL
 - definición 487
 - mandatos de configuración 490
 - requisitos 488
 - utilización de 487
 - Servidor BOOTP 511
 - servidor de autenticación
 - ACE/Server 256
 - definición 256

- servidor de nombres de dominio dinámico (DDNS)
 - descripción 494
- servidor DHCP 507, 539
 - clientes DHCP especiales 511
 - conceptos 512
 - configuración de ejemplo 530
 - introducción 507
 - movimiento de clientes 509
 - número de servidores DHCP 510
 - opciones
 - básicas, proporcionadas al cliente 517
 - específicas de IBM 528
 - extensiones DHCP 524
 - formatos 515
 - parámetros de aplicaciones y servicios 522
 - parámetros de capa de enlace por interfaz 522
 - parámetros de capa IP por interfaz 521
 - parámetros de capa IP por sistema principal 520
 - parámetros de TCP 522
 - proveedor 528
 - opciones del servidor, modificación 509
 - operación de DHCP 507
 - períodos de tiempo de alquiler 512
 - renovación de alquileres 509
 - servidor DHCP y parámetros de alquiler 515
 - servidor DHCP, único 510
 - Servidores BOOTP 511
 - servidores DHCP, múltiples 510
 - terminología 512
- Servidor TN3270E 155
- set
 - mandato de configuración de la Conversión de direcciones de red 483
 - mandato de configuración de NAT 483
 - mandato de configuración de Redireccionamiento de WAN 83, 89
 - mandato de configuración de seguridad de IP 402
 - mandato de configuración de TSF 599
 - mandato de supervisión de seguridad de IP 422
 - mandato de supervisión de TSF 607
 - mandatos de configuración de QoS de la interfaz ATM 297
 - mandatos de configuración de QoS de LE Client 293
 - mandatos de configuración de servidor DHCP 563
 - parámetros del subsistema de codificación 231
- set circuit defaults
 - mandato de configuración de reserva de ancho de banda 48
- set-action
 - mandato de actualización de filtrado MAC 67
- show
 - mandato de configuración de reserva de ancho de banda 48
- sistema de colas de prioridad
 - descripción 6

- Sistema de reserva de ancho de banda (BRS)
 - descripción 1
 - Elegibilidad de eliminación (DE) 4
 - Filtrado de números de puerto TCP/UDP 9
 - utilización del proceso de bits de precedencia de IP Versión 4 10
- stats
 - mandato de supervisión de seguridad de IP 412, 422
- submandatos de actualización
 - mandato de configuración de Filtrado MAC 57
- subsistema de codificación
 - configuración 229
 - supervisión 229, 231
- supervisión 387
 - cifrado
 - para frame relay 283
 - para PPP 280
 - compresión de datos en enlaces Frame Relay 245
 - compresión de datos en enlaces PPP 243
 - mandatos de supervisión de TSF 601
 - MPPE
 - para PPP 282
 - seguridad de IP (IPv4) 410
 - seguridad de IP manual (IPv6) 423
- sustained-cell-rate
 - QoS 288

T

- tabla de dependencias 180
- TACACS 614
- tag
 - mandato de configuración de reserva de ancho de banda 49
- talk
 - mandato OPCON 495, 503, 539, 572, 591, 601
- traffic-type
 - parámetro de QoS 287
- translate
 - mandato de configuración de la Conversión de direcciones de red 484
 - mandato de configuración de NAT 484
- TSF
 - actualizaciones de la antememoria de archivos 581
 - configuración 591
 - configuración de ejemplo 584
 - configuración del servidor BootP/DHCP 583
 - configuración del servidor para TSF 583
 - pasos de la configuración 581
 - utilización de 577
 - utilización de RFS 580
 - utilización de TFTP 580
 - visión general 578
- túnel en túnel para seguridad de IP 375

túneles seguros 367

U

untag

- mandato de configuración de reserva de ancho de banda 49

update

- mandato de configuración de filtrado MAC 63

use circuit defaults

- mandato de configuración de reserva de ancho de banda 50

utilización de

- dial-in access server 487

utilización de Antememoria del servidor de la web 169

utilización de Restauración de WAN 71

utilización del Proxy HTTP 174

V

validar pcr-of-best-effort-vccs

- QoS 290

VCRM

- configuración y supervisión 609

Vector de respuesta de mandato 184

visión general

- de compresión 237

- Redireccionamiento de WAN 71

- Restauración de WAN 71

visión general de la Antememoria del servidor de la web 169

visión general del gestor de control de antememoria externa 179

voa a través de frame relay (VOFR) 33

Hoja de Comentarios

Nways Multiprotocol Access Services
Características de utilización y
configuración
Versión 3.3

Número de Publicación SC10-3435-00

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



Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.

SC10-3435-00

