Access Integration Services

Utilización y configuración de las características Versión 3.3

SC10-3437-00

Access Integration Services

Utilización y configuración de las características Versión 3.3

SC10-3437-00

Nota

Antes de utilizar este documento, lea la información general que hay en “Avisos” en la página xv.

Primera edición (Junio de 1999)

Esta edición es aplicable a la Versión 3.3 de IBM Access Integration Services y a todos los releases y modificaciones ulteriores hasta que se indique lo contrario en nuevas ediciones o boletines técnicos.

Puede solicitar publicaciones a través de su representante o distribuidor IBM. En la dirección que figura a continuación no se distribuyen publicaciones.

IBM le anima a hacer comentarios. Al final de esta publicación verá una hoja para los comentario del lector. Si no la encuentra, puede dirigir sus comentarios a:

IBM S.A.
Avda. Diagonal 571
08029 Barcelona
España

Cuando envía información a IBM, otorga a IBM un derecho no exclusivo para utilizar o distribuir la información de la manera que IBM crea más adecuada sin incurrir por ello en ninguna obligación con usted.

Contenido

Avisos . . . . . **xv**

Aviso a los usuarios de las versiones en línea de esta publicación . . . . . **xvii**

Marcas registradas . . . . . **xix**

Prefacio . . . . . **xxi**
A quién está dirigido este manual xxi
Acerca del software xxi
Convenios utilizados en este manual xxii
Visión general de la biblioteca xxii
Resumen de los cambios correspondientes a la biblioteca software IBM 2212 xxiv
Obtención de ayuda xxv
Salida de un entorno de nivel inferior xxv

Capítulo 1. Utilización de la reserva de ancho de banda y de colas de prioridad 1
Sistema de reserva de ancho de banda 1
Reserva de ancho de banda sobre Frame Relay . . 3
Soporte de colas 4
Elegibilidad para ser descartado 4
Definiciones de circuito por omisión para manejar clases de tráfico 4
Configuración de BRS para voz a través de Frame Relay 5
Colas de prioridad 5
Colas de prioridad sin reserva de ancho de banda 6
Configuración de las clases de tráfico 6
BRS y filtros 7
Filtrado de direcciones MAC e identificadores . 7
Filtrado de número de puerto TCP/UDP 8
Filtrado de bits TOS de IPv4 9
Proceso de bits de precedencia de IP versión 4 para tráfico SNA en túneles seguros IP y fragmentos secundarios 10
Filtrado de SNA y APPN para tráfico que se transmite por un puente 11
Orden de precedencia del filtrado 12
Configuraciones de ejemplo 12
Uso de las definiciones de circuito por omisión para manejar clases de tráfico de circuitos Frame Relay 13

Capítulo 2. Configuración y supervisión de la reserva de ancho de banda **25**
Visión general de la configuración de la reserva de ancho de banda 25
Mandatos de configuración de la reserva de ancho de banda 26
Activate-IP-precedence-filtering 30
Add-circuit-class 31
Add-class 31
Assign 33
Assign-circuit 36
Change-circuit-class 37
Change-class 37
Circuit 37
Clear-block 38
Create-super-class 38
Deactivate-IP-precedence-filtering 39
Deassign 39
Deassign-circuit 39
Default-circuit-class 39
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 47
Show 48
Tag 48
Untag 49
Use-circuit-defaults 49
Acceso al indicador de supervisión de la reserva de ancho de banda 50
Mandatos de supervisión de la reserva de ancho de banda 50
Circuit 51
Clear 52
Clear-Circuit-Class 52
Counters 52
Counters-circuit-class 53
Interface 53
Last 54
Last-circuit-class 54

Capítulo 3. Utilización del filtrado MAC 55
Filtros MAC y tráfico DLSw 55
Parámetros del filtrado MAC 56
Parámetros de los elementos filtro 56
Parámetros de las listas de filtros 56
Parámetros de los filtros 56
Utilización de identificadores del filtrado MAC 57

Capítulo 4. Configuración y supervisión del filtrado MAC **59**
Acceso al indicador de configuración del filtrado MAC 59
Mandatos de configuración del filtrado MAC . . . 59

Attach . . . 60
Create . . . 60
Default . . . 60
Delete . . . 61
Detach . . . 61
Disable . . . 62
Enable . . . 62
List . . . 62
Move . . . 63
Reinit . . . 63
Set-Cache . . . 63
Update . . . 63
Submandatos de actualización . . . 63
Add . . . 64
Delete . . . 65
List . . . 65
Move . . . 66
Set-Action . . . 66
Acceso al indicador de supervisión del filtrado MAC . . . 67
Mandatos de supervisión del filtrado MAC . . . 67
Clear . . . 67
Disable . . . 68
Enable . . . 68
List . . . 68
Reinit . . . 69

Capítulo 5. Utilización de la restauración de WAN . . . 71
Visión general de las características restauración de WAN, redireccionamiento de WAN y marcación por desbordamiento . . . 71
restauración de WAN . . . 71
redireccionamiento de WAN . . . 72
marcación por desbordamiento . . . 73
Antes de empezar . . . 73
Procedimiento de configuración de la restauración de WAN . . . 74
Configuración del circuito de marcación secundario . . . 74

Capítulo 6. Configuración y supervisión de la restauración de WAN 77
Mandatos de configuración de la restauración de WAN, del redireccionamiento de WAN y de la marcación por desbordamiento . . . 77
Add . . . 78
Disable . . . 79
Enable . . . 80
List . . . 81
Remove . . . 81
Set . . . 82
Acceso al proceso de supervisión de interfaces de la restauración de WAN . . . 85
Mandatos de supervisión de la restauración de WAN . . . 85
Clear . . . 86
Disable . . . 86
Enable . . . 87
Set . . . 88
List . . . 91

Capítulo 7. La característica de redireccionamiento de WAN . . . 97
Visión general del redireccionamiento de WAN . . 97
Marcación por desbordamiento . . . 98
Configuración del redireccionamiento de WAN . . 99
Ejemplo de configuración del redireccionamiento de WAN . . . 99

Capítulo 8. Utilización de la característica Network Dispatcher . . 105
Visión general de Network Dispatcher . . . 105
Reparto del tráfico TCP y UDP utilizando Network Dispatcher . . . 106
Alta disponibilidad de Network Dispatcher . . . 107
Detección de anomalías . . . 108
Sincronización de bases de datos . . . 108
Estrategia de recuperación . . . 109
Toma de control de IP . . . 109
Configuración de Network Dispatcher . . . 109
Pasos para la configuración . . . 111
Utilización de Network Dispatcher con el servidor TN3270 . . . 116
Puntos clave para la configuración . . . 116
LU explicitas y Network Dispatcher . . . 117
Utilización de Network Dispatcher con Antememoria de servidor Web . . . 117
Utilización de Network Dispatcher con eNetwork Host On-Demand Client Cache . . . 118
Utilización de Network Dispatcher con la función SHAC (Scaleable High Availability Cache) . . . 118

Capítulo 9. Configuración y supervisión de la característica Network Dispatcher . . . 121
Acceso a los mandatos de configuración de Network Dispatcher . . . 121
Mandatos de configuración de Network Dispatcher . . . 121
Add . . . 121
Clear . . . 128
Disable . . . 128
Enable . . . 129
List . . . 131
Remove . . . 132
Set . . . 135
Acceso a los mandatos de supervisión del Network Dispatcher . . . 140
Mandatos de supervisión del Network Dispatcher 141
List . . . 141
Quiesce . . . 143
Report . . . 144
Status . . . 145
Switchover . . . 148
Unquiesce . . . 148

Capítulo 10. Configuración y supervisión de Host On-Demand Client Cache para eNetwork de IBM 151

Configuración de Host On-Demand Client Cache 151
Acceso al entorno de configuración de Host On-Demand Client Cache 155
Mandatos de Host On-Demand Client Cache . . 155
- Activate 156
- Add 156
- Delete 156
- List 157
- Modify 158

Acceso al entorno de supervisión de Host On-Demand Client Cache 159
Mandatos de supervisión de Host On-Demand Client Cache 159
- Activate 159
- Clear 160
- Enable 160
- Delete 160
- Disable 161
- List 161
- Modify 163

Capítulo 11. Utilización de la Antememoria de servidor Web 165

Visión general de la Antememoria de servidor Web 165
- Almacenamiento en antememoria 167

Utilización del Proxy HTTP 170
Antememoria escalable de alta disponibilidad . . 172
Visión general del gestor de control de antememoria externa 174
- Tabla de dependencias 175
- Protocolo de control de la antememoria externa 176
- Formatos de los vectores del protocolo de control de la antememoria externa (ECCP) . . 179

Capítulo 12. Configuración y supervisión de la Antememoria de servidor Web 201

Configuración de la Antememoria de servidor Web 201
Acceso al entorno de la Antememoria de servidor Web 208
Mandatos de la Antememoria de servidor Web . 208
- Activate 208
- Add 208
- Delete 209
- List 210
- Modify 211

Acceso al entorno de supervisión de la Antememoria de servidor Web 215
Mandatos de supervisión de la Antememoria de servidor Web 215
- Activate 216
- Clear 216
- Enable 217
- Delete 217
- Disable 218
- List 218
- Modify 221

Capítulo 13. Configuración y supervisión del subsistema de codificación 223

Configuración del subsistema de codificación . . 223
- List 224
- Set 225

Supervisión del subsistema de codificación . . . 225
- List 226

Capítulo 14. Configuración y supervisión de la compresión de datos 231

Visión general de la compresión de datos 231
Conceptos de la compresión de datos 231
- Nociones básicas sobre compresión de datos . 232
- Consideraciones 234

Configuración y supervisión de la compresión de datos para enlaces PPP 236
- Configuración de la compresión de datos para enlaces PPP 237
- Supervisión de la compresión de datos para enlaces PPP 238

Configuración y supervisión de la compresión de datos para enlaces Frame Relay 239
- Configuración de la compresión de datos para enlaces Frame Relay 239
- Supervisión de la compresión de datos para enlaces Frame Relay 241
- Ejemplo: Supervisión de la compresión para una interfaz o circuito Frame Relay 242

Capítulo 15. Utilización de la autenticación local o remota 245

Utilización de la seguridad de autenticación, autorización y contabilidad (AAA) 245
- ¿Qué es la seguridad AAA? 245
- Utilización de PPP 246
- Protocolos válidos de seguridad PPP 246
- Utilización del inicio de sesión 247
- Protocolos válidos de seguridad de inicio de sesión y administración 248
- Utilización de túneles 248
- Protocolos válidos de seguridad de túneles . . 248
- Normas sobre las contraseñas 249

Explicación de los servidores de autenticación . . 249
- Soporte de identificación de seguridad 250

Capítulo 16. Configuración de la autenticación 253

Acceso al indicador de configuración de la autenticación 253
Mandatos de configuración de la autenticación . 253
- Disable 253
- List 253
- Login 255

Nets-info 257
Password-rules 257
PPP 259
Servers 261
Set 264
Tunnel 265
User-profiles 266

Capítulo 17. Utilización y configuración de los protocolos de cifrado 271
Cifrado PPP mediante el Protocolo de control del cifrado 271
Configuración del cifrado ECP para PPP . . . 271
Supervisión del cifrado ECP para PPP 272
Cifrado de punto a punto de Microsoft (MPPE) . 272
Configuración de MPPE 273
Supervisión de MPPE 273
Configuración del cifrado en las interfaces de Frame Relay 274
Supervisión del cifrado en las interfaces de Frame Relay 274

Capítulo 18. Utilización de la función de política 275
Visión general de la política 275
Decisión y aplicación de una política 275
Objetos de política 278
Interacción de la base de datos de políticas y LDAP 283
Esquema de política 285
Generación de normas 287
Ejemplos de configuración 288
Política IPSec/ISAKMP con QOS 288
Política de sólo IPSec/ISAKMP 300
Desconexión de todo el tráfico público (norma de filtro) 303
Configuración y habilitación del motor de búsqueda de políticas LDAP 307

Capítulo 19. Configuración y supervisión de la función de política 311
Acceso al indicador de configuración de la política 311
Mandatos de configuración de la política 311
Add 312
Change 324
Copy 324
Delete 324
Disable 324
Enable 324
List 324
Mandatos de configuración del servidor de políticas de LDAP 325
Disable LDAP 325
Enable LDAP 325
Set Default-Policy 325
Set LDAP 327
Set Refresh 328
Acceso al indicador de supervisión de la política 329
Mandatos de supervisión de la política 329
Disable 330
Enable 330
Reset 330
Search 330
Status 331
List 331
Test 332

Capítulo 20. Utilización de la seguridad IP 335
Visión general de la seguridad IP 335
Utilización de los túneles protegidos 335
Conceptos de seguridad IP 336
Terminología de seguridad IP 336
Cabecera de autenticación de IP 338
Carga útil de seguridad de encapsulación de IP 339
Utilización de AH y ESP 339
Asociaciones de seguridad 340
Modalidad de túnel y modalidad de transporte 340
Modalidad de túnel en túnel 342
Descubrimiento de la unidad de transmisión máxima de la vía de acceso 343
Diagrama de una red con un túnel de seguridad IP 344
Utilización del Intercambio de claves de Internet 345
Fases del Intercambio de claves de Internet . . 345
Negociación de un túnel de seguridad IP . . . 346
Utilización de la Infraestructura de claves públicas 347
Configuración de PKI 348
Utilización de la seguridad IP manual (IPv4) . . 352
Utilización de la seguridad de IP manual (IPv6) . 352

Capítulo 21. Configuración y supervisión de la seguridad IP 353
Configuración del intercambio de claves en Internet (IPv4) 353
Configuración de la infraestructura de claves públicas (IPv4) 354
Obtención de un certificado 354
Mandatos de configuración de la infraestructura de claves públicas 355
Add 355
Change 355
Delete 356
List 357
Configuración de la seguridad IP manual (IPv4) 358
Configuración de los algoritmos 358
Configuración de las claves de cifrado 359
Acceso al entorno de configuración de la seguridad IP 359
Mandatos de configuración de seguridad IP manual 359
Add Tunnel 359
Change Tunnel 364
Delete Tunnel 365
Disable 365
Enable 366
List 366
Set 367

Configuración de un túnel manual (IPv4) 368
Configuración del túnel para el direccionador A 368
Configuración del túnel para el direccionador B 368
Ejemplo: Configuración manual de un túnel de seguridad IP con ESP 368
Ejemplo: Configuración manual de un túnel de seguridad IP con ESP y ESP-NULL 369
Configuración de la seguridad IP manual (IPv6) 369
Configuración de los algoritmos 370
Configuración de las claves de cifrado 370
Acceso al entorno de configuración de la seguridad IP 370
Mandatos de configuración de seguridad IP manual 371
Configuración de un túnel manual (IPv6) 371
Creación del túnel de seguridad IP para el direccionador A 371
Configuración de filtros de paquetes para el direccionador A 372
Configuración de las normas del control de acceso de filtros de paquetes para el direccionador A 372
Restablecimiento de la seguridad IP y de IP en el direccionador A 373
Creación del túnel de seguridad IP para el direccionador B 373
Configuración de filtros de paquetes para el direccionador B 373
Configuración de las normas de control de acceso del filtro de paquetes para el direccionador B 373
Restablecimiento de la seguridad IP y de IPv6 en el direccionador B 374
Ejemplo: Configuración de un túnel de seguridad IP con ESP 374
Ejemplo: Configuración de un túnel de seguridad IP con ESP y ESP-NULL 375
Supervisión de la seguridad IP manual (IPv4) . . 375
Acceso al entorno intercambio de claves en Internet 375
Mandatos de supervisión de intercambio de claves en Internet 375
Acceso al entorno de la infraestructura de claves públicas (IPv4) 377
Mandatos de supervisión de la infraestructura de claves públicas 378
Acceso al entorno de supervisión de la seguridad IP (IPv4) 381
Mandatos de supervisión de la seguridad IP (IPv4) 381
Supervisión de la seguridad IP manual (IPv6) . . 387
Acceso al entorno de supervisión de la seguridad IP 387
Mandatos de supervisión de la seguridad IP (IPv6) 387

Capítulo 22. Utilización de la función de servicios diferenciados 389
Visión general de los servicios diferenciados . . . 389
Terminología de los servicios diferenciados . . . 392
Configuración de los servicios diferenciados . . . 392

Capítulo 23. Configuración y supervisión de la función de servicios diferenciados 395
Acceso al indicador de configuración de los servicios diferenciados 395
Mandatos de configuración de los servicios diferenciados 395
Delete 396
Disable 396
Enable 396
List 397
Set 398
Acceso al entorno de supervisión de los servicios diferenciados 400
Mandatos de supervisión de los servicios diferenciados 401
Clear 401
DScache 401
List 402

Capítulo 24. Utilización de túneles de capa 2 (L2TP, PPTP, L2F) 407
Visión general de L2TP 407
Términos de L2TP 408
Funciones que reciben soporte 408
Consideraciones de tiempo 410
Consideraciones sobre LCP 410
Configuración de túneles de capa 2 410

Capítulo 25. Configuración y supervisión de los protocolos de túnel de capa 2 417
Acceso al indicador de configuración de la interfaz de L2T 417
Mandatos de configuración de la interfaz de túneles L2 417
Disable 418
Enable 418
Encapsulator 418
List 418
Set 418
Acceso al indicador de configuración de la función de túneles L2 419
Mandatos de configuración de la función de túnel L2 419
Add 420
Disable 420
Enable 421
Encapsulator 422
List 422
Set 423
Acceso al indicador de supervisión de túneles L2 424
Mandatos de supervisión de túneles L2 425
Call 425
Kill 428
Memory 428
Start 428
Stop 428

Tunnel 429

Capítulo 26. Utilización de la conversión de direcciones de red (NAT) 433

Conversión de puertos y direcciones de red . . . 434
Correlaciones de direcciones estáticas 435
Correlación de direcciones estáticas NAT . . . 435
Correlación de direcciones estáticas NAPT . . 435
Establecimiento de filtros de paquetes y de reglas de control de acceso para NAT 436
Ejemplo: Configuración de NAT con filtros IP y reglas de control de acceso 436

Capítulo 27. Configuración y supervisión de la conversión de direcciones de red 441

Acceso al entorno de configuración de la conversión de direcciones de red 441
Mandatos de configuración de la conversión de direcciones de red 441
Change 442
Delete 442
Disable 443
Enable 443
List 443
Map 444
Reserve 445
Reset 447
Set 447
Translate 448
Acceso al entorno de supervisión de la conversión de direcciones de red 448
Mandatos de supervisión de la conversión de direcciones de red 448
List 449
Reset 450

Capítulo 28. Utilización de un servidor Acceso de marcación a las LAN (DIALs) 451

Antes de la utilización de Dial-In-Access 453
Configuración de Dial-In Access 453
Configuración de interfaces de establecimiento de conexión de entrada 453
Antes de la configuración de interfaces de establecimiento de conexión de salida 456
| Utilización del módem nulo 456
Configuración de interfaces de establecimiento de conexión de salida 456
Antes de la configuración de los parámetros de DIALs globales 458
Direcciones IP proporcionadas por el servidor 458
Protocolo de configuración dinámica de sistemas principales (DHCP) 459
Servidor de nombres de dominio dinámico (DDNS) 461

Capítulo 29. Configuración de DIALs 463

Acceso al entorno de configuración global de DIALs 463
Mandatos de configuración global de DIALs . . 463
Add 464
Delete 465
Disable 465
Enable 466
List 467
Set 469
Acceso al entorno de supervisión global de DIALs 472
Mandatos de supervisión global de DIALs 472
Clear 472
List 473
Reset 475
Mandatos de configuración de la interfaz de establecimiento de conexión de salida 476
Set 476
Supervisión de interfaces de establecimiento de conexión de entrada 476
Supervisión de interfaces de establecimiento de conexión de salida 476
Clear 477
List 477

| Capítulo 30. Utilización del Servidor | DHCP 479

| Introducción a DHCP 479
| Operación DHCP 479
| Renovaciones de cesiones 481
| Movimiento del cliente 481
| Modificación de las opciones de servidor . . . 481
| Número de servidores DHCP 482
| Un único servidor DHCP 482
| Varios servidores DHCP 482
| Servidores BOOTP 483
| Clientes DHCP especiales 483
| Tiempos de cesión 484
| Conceptos y terminología 484
| Parámetros de servidor DHCP y de cesión 487
| Opciones DHCP 487
| Formatos de opción 487
| Opciones base proporcionadas al cliente . . . 489
| Parámetros de capa IP por opciones de sistema principal 491
| Parámetros de capa IP por opciones de interfaz 492
| Parámetros de capa de enlace por opciones de interfaz 493
| Opciones de parámetros TCP 493
| Opciones de parámetros de aplicaciones y servicios 494
| Opciones de extensiones DHCP 495
| Opciones específicas de IBM 499
| Opciones de proveedor 499
| Configuración de IP para DHCP 500
| Adición de una dirección IP 500
| Utilización del acceso simple a Internet del IP 501
| Configuración de ejemplo del servidor DHCP . . 501
| Archivo de texto ASCII 501
| Configuración de OPCON (talk 6) 503

Capítulo 31. Configuración y supervisión del servidor DHCP 509
Acceso al entorno de configuración del servidor DHCP 509
Mandatos de configuración del servidor DHCP . 509
Add 510
Change 516
Delete 521
Disable 524
Enable 525
List 525
Set 532
Acceso al entorno de supervisión del servidor DHCP 541
Mandatos de supervisión del servidor DHCP . . 541
Disable 542
Enable 542
List 542
Reset 542
Request 543

Capítulo 32. Utilización de la Thin Server Feature 547
Visión general de la Network Station 547
Visión general de la Thin Server Feature 547
Soporte de BootP/DHCP 549
Protocolos utilizados para comunicar con Network Stations 550
Utilización de RFS 550
Utilización de TFTP 550
Utilización de NFS 550
Actualizaciones de antememorias de archivos . . 551
Configuración del entorno del Thin Server 551
Recomendaciones de configuración 551
Configuración del servidor BootP/DHCP . . . 552
Configuración del servidor para el entorno del Thin Server 553
Configuración de BootP Relay 553
Configuración de la dirección IP interna . . . 553
Configuración de la TSF 553
Ejemplo de configuración 553
Configuración del AS/400 554
Configuración del IBM 2212 (TSF) 556

Capítulo 33. Configuración y supervisión de la Thin Server Function 559
Acceso al entorno de configuración de la TSF . . 559
Mandatos de configuración de la TSF 559
Add 559
Delete 565
List 566
Modify 566
Set 567
Acceso al entorno de supervisión de la TSF . . . 569
Mandatos de supervisión de la TSF 569
Delete 569
Flush 570
List 570
Refresh 573
Reset 574
Restart 574
Set 574

Capítulo 34. Configuración y supervisión del VCRM 575
Acceso al entorno de configuración del VCRM . 575
Acceso al entorno de supervisión del VCRM . . 575
Mandatos de supervisión del VCRM 576
Clear 576
Queue 576

Capítulo 35. Utilización de los adaptadores de voz 579
Visión general del adaptador de voz 579
Configuración del Nuera F200 para la comunicación con un adaptador de voz del 2212 580
Configuración de un plan de marcación . . . 582
Configuración del puerto de voz 2212 para la comunicación con el Nuera F200 583
Comunicación sin utilizar un Nuera F200 584
Comunicación de 2212 a 2212 584
Direccionamiento de llamadas locales 584

Capítulo 36. Configuración y supervisión de los adaptadores de voz 587
Acceso al entorno de configuración de la característica de voz 587
Mandatos de configuración del adaptador de voz 587
Add 588
Delete 591
List 591
Modify 593
Reorder-Call-Rule 593
Set 593
Mandatos de configuración de una red de voz . 597
List 597
Set 598
Acceso al entorno de supervisión del adaptador de voz 600
Mandatos de supervisión del adaptador de voz . 600
Calls 601
Status 602
Trace Call 604

Apéndice A. Atributos de la seguridad AAA remota 605
Radius 605
Palabras clave 605
TACACS+ 606

Apéndice B. Lista de Abreviaturas . 607

Glosario 617

Índice 643

Figuras

1. Relación entre la clase de tráfico y la cola de prioridad de la clase de tráfico para una interfaz PPP en BRS 2
2. Relación entre la clase de circuito y la clase de tráfico para una interfaz Frame Relay en BRS 2
3. Redireccionamiento de WAN 98
4. Ejemplo de configuración del redireccionamiento de WAN 100
5. Ejemplo de Network Dispatcher configurado con un único cluster y 2 puertos 109
6. Ejemplo de Network Dispatcher configurado con 3 clusters y 3 URL 110
7. Ejemplo de Network Dispatcher configurado con 3 clusters y 3 puertos 111
8. Configuración de Alta disponibilidad de Network Dispatcher 112
9. Dos antememorias con Network Dispatcher, un cliente y un servidor final. 119
10. Network Dispatcher sin Antememoria de servidor Web 166
11. Network Dispatcher con Antememoria de servidor Web y sin acierto en la antememoria 166
12. Network Dispatcher con Antememoria de servidor Web y con acierto en la antememoria 167
13. Encontrada petición hecha a la antememoria 172
14. Petición reenviada a la antememoria responsable 173
15. Petición reenviada al servidor final 173
16. Petición reenviada a la antememoria responsable y no encontrada 174
17. Vector de respuesta de mandatos 179
18. Formato de un subvector 183
19. Formato de un subcampo 197
20. Ejemplo de compresión de datos bidireccional con diccionarios de datos . . 234
21. Ejemplo de configuración de la compresión para un enlace PPP 237
22. Supervisión de la compresión para una interfaz PPP 239
23. Ejemplo de configuración de la compresión para un enlace Frame Relay 240
24. Nombre de usuario y código de paso de la identificación de seguridad 250
25. Código de paso de la identificación de seguridad con la seña siguiente 250
26. Flujo de paquetes de IP y base de datos de políticas 276
27. Relación de los objetos de configuración de una política 283
28. Protección del tráfico a través de Internet . 284
29. Estructura del esquema de política 286
30. Configuración de IPSec/ISAKMP con QOS 289
31. Configuración de IPSec y utilización de una definición anterior 300
32. Creación de un mensaje autenticado por MD5 de HMAC 339
33. Formato de datagramas de AH protegida . 341
34. Formato de datagramas de ESP protegido . 341
35. Anidación de ESP dentro de un túnel de AH 342
36. Paquete de L2TP de IPSec protegido . . . 342
37. Red con IPSec y NAT 344
38. Vía de acceso de paquetes de datos de DiffServ 389
39. Relación entre almacenamientos intermedios, colas y planificador 391
40. Ejemplo de red L2TP 407
41. Red en la que se ejecuta NAT 434
42. Red en la que se ejecuta NAT 437
43. Un ejemplo de Servidor DIALs que ofrece soporte a establecimiento de conexión de entrada 452
44. Un ejemplo de Servidor DIALs que ofrece soporte a establecimiento de conexión de salida, ... 453
45. Adición de una interfaz de establecimiento de conexión de entrada 455
46. Conceptos de ámbito 485
47. Estación de red remota sin Thin Server . . 549
48. Estación de red remota con un Thin Server 549
49. Ejemplo de configuración de la TSF 554
50. Comunicación entre los puertos de voz Nuera F200 y 2212 580
51. Configuración de la información del proceso de llamadas del puerto de voz 581

Tablas

1. Resumen de los mandatos de configuración de la reserva de ancho de banda (disponibles desde el indicador BRS Config>) 27
2. Mandatos de configuración de interfaz de BRS disponibles desde el indicador BRS [i #] Config> para interfaces Frame Relay 28
3. Mandatos para manejar clases de tráfico de BRS 29
4. Resumen de mandatos de supervisión de la reserva de ancho de banda 51
5. Resumen de mandatos de configuración del filtrado MAC 59
6. Resumen de submandatos de actualización . 64
7. Resumen de mandatos de supervisión del filtrado MAC 67
8. Resumen de los mandatos de configuración de la restauración de WAN 77
9. Mandatos de supervisión de la restauración de WAN 85
10. Mandatos para cambiar el nombre del dispositivo bucle de retorno (lo0) para Dispatcher 114
11. Mandatos para eliminar rutas en varios sistemas operativos 116
12. Mandatos de configuración de Network Dispatcher 121
13. Nombres y números de puerto del asesor . 122
14. Límites a la configuración de parámetros . 128
15. Mandatos de supervisión de Network Dispatcher 141
16. Resumen de los mandatos de configuración de Host On-Demand Client Cache 155
17. Resumen de mandatos de supervisión de Host On-Demand Client Cache 159
18. Resumen de mandatos de configuración de la Antememoria de servidor Web 208
19. Resumen de los mandatos de supervisión de la Antememoria de servidor Web 215
20. Mantados de configuración del ES 224
21. Mandato de supervisión del ES 226
22. Mandatos de configuración de la compresión de datos para PPP 237
23. Mandatos de supervisión de la compresión de datos para PPP 238
24. Mandatos de configuración de la compresión de datos 241
25. Mandatos de supervisión de la compresión de datos para Frame Relay 241
26. Establecer protocolos de seguridad PPP . . 247
27. Establecer protocolos de seguridad de inicio de sesión 248
28. Establecer protocolos de seguridad de túneles 249
29. Mandatos de configuración de la autenticación 253
30. Submandatos de login 255
31. Submandatos de login 257
32. Submandatos de PPP 259
33. Submandatos de Server 261
34. Submandatos de tunnel 265
35. Mandatos de configuración de perfil de usuario 266
36. Consultas de fase 1 de IKE y decisiones recibidas 277
37. Consultas de fase 2 de IKE y decisiones recibidas 278
38. Mandatos de configuración de la política . 311
39. Mandatos de configuración de LDAP . . . 325
40. Mandatos de supervisión de la política . . 329
41. Algoritmos configurados con varias políticas de túneles 358
42. Resumen de mandatos de configuración de seguridad IP 359
43. Algoritmos configurados con varias políticas de túneles 370
44. Resumen de los mandatos de supervisión de IKE 375
45. Resumen de los mandatos de supervisión de PKI 378
46. Resumen de mandatos de supervisión de la seguridad IP 381
47. Mandatos de configuración de DiffServ . . 395
48. Mandatos de supervisión de DiffServ . . . 401
49. Mandatos de configuración de la interfaz de túneles L2 417
50. Mandatos de configuración de la función de túnel L2 419
51. Mandatos de supervisión de túneles L2 . . 425
52. Mandatos de configuración de NAT 441
53. Mandatos de supervisión de NAT 449
54. Mandatos de configuración global de DIALs 463
55. Mandatos de supervisión global DIALs . . 472
56. Mandatos de configuración de la interfaz de establecimiento de conexión de salida . . . 476
57. Mandatos de configuración de interfaces de establecimiento de conexión de salida . . . 477
58. Resumen de mandatos de configuración del servidor DHCP 509
59. Resumen de mandatos de supervisión del servidor DHCP 541
60. Resumen de mandatos de configuración de la TSF 559
61. Resumen de mandatos de supervisión de la TSF 569
62. Mandatos de supervisión del VCRM . . . 576
63. Resumen de los mandatos de configuración de la característica de voz 587
64. Resumen de mandatos del puerto de voz . 597
65. Resumen de mandatos de supervisión del adaptador de voz 600

Avisos

Las referencias que se hacen 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 IBM realiza operaciones. Las referencias a un producto, programa o servicio de IBM no pretenden afirmar ni dar a entender que únicamente pueda utilizarse dicho producto, programa o servicio de IBM. Puede utilizarse en su lugar cualquier otro producto, programa o servicio funcionalmente equivalente que no vulnere ninguno de los derechos de propiedad intelectual de IBM. Son responsabilidad del usuario la verificación y la evaluación del funcionamiento junto con otros productos, excepto aquéllos expresamente indicados por IBM.

IBM puede tener patentes o solicitudes de patente pendientes que cubran los temas tratados en este documento. La posesión de este documento no confiere ninguna licencia sobre dichas patentes. Puede enviar consultas sobre las licencias, por escrito, 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, bajo los términos del Contrato de Cliente IBM.

Este documento no está pensado para utilizarse en la fase de producción y se entrega tal cual, sin garantías de ninguna clase, por lo que aquí se renuncia explícitamente a todas las garantías, incluidas las de comerciabilidad e idoneidad para un fin concreto.

Aviso a los usuarios de las versiones en línea de esta publicación

Para las versiones en línea de esta publicación, posee usted autorización para:

- Copiar, modificar e imprimir la documentación contenida en el medio de distribución en línea para usarla dentro de su empresa, siempre y cuando reproduzca en cada copia o copia parcial el aviso de derechos de propiedad intelectual, todas las declaraciones de advertencias y las demás declaraciones necesarias.
- Transferir la copia original y no alterada de la documentación cuando transfiera el producto de IBM relacionado (que pueden ser máquinas de su propiedad o programas, si los términos de la licencia del programa permiten una transferencia). Es preciso que, a la vez, destruya todas las demás copias de la documentación.

Es usted responsable del pago de los impuestos que puedan derivarse de esta autorización, incluidos los impuestos sobre bienes personales.

SE RENUNCIA A TODAS LAS GARANTÍAS, EXPLÍCITAS O IMPLÍCITAS, INCLUIDAS, PERO SIN LIMITARSE A ELLAS, LAS GARANTÍAS DE COMERCIABILIDAD E IDONEIDAD PARA UN FIN CONCRETO.

Algunas jurisdicciones no permiten la exclusión de las garantías implícitas, por lo que puede ser que la renuncia anterior no sea aplicable a su caso.

Si usted incumple los términos descritos más arriba, se podrá dar por finalizada esta autorización, en cuyo caso, deberá destruir la documentación legible por 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	

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

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

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

Prefacio

Este manual contiene la información que necesitará para utilizar la interfaz de usuario del direccionador con el fin de configurar las características instaladas en el IBM 2212 y poder trabajar con ellas. Es posible que un determinado IBM 2212 no dé soporte a todas las características que se describen en este manual. Se informa de que una característica es específica de un dispositivo determinado mediante:

- Un aviso en el capítulo o apartado adecuado
- Una sección en el prefacio, donde se listan todas las características y los dispositivos que les dan soporte.

Este manual trata del IBM 2212 y se hace referencia a él como "direccionador" o como "dispositivo". Los ejemplos del manual representan la configuración de un IBM 2212, pero la salida real que vea puede ser distinta. Los ejemplos son orientativos de lo que verá durante la configuración del dispositivo.

A quién está dirigido este manual

Este manual está dirigido a las personas que instalan y gestionan redes de ordenadores. Aunque puede ser de gran ayuda tener experiencia en el hardware y el software de alguna red de ordenadores, para utilizar el software de los protocolos no es necesario tener conocimientos de programación.

Para obtener información adicional: pueden realizarse cambios en la documentación después de que se hayan impreso las publicaciones. Si hay información adicional disponible o si es necesario realizar cambios una vez impresas las publicaciones, dichos cambios estarán en un archivo (llamado README) del disquete 1 de los disquetes del programa de configuración. Puede ver el archivo con un editor de texto ASCII.

Acerca del software

IBM Access Integration Services es el software que da soporte a IBM 2212 (programa bajo licencia número 5639-F73). Este software tiene estos componentes:

- El código base, que consta de:
  - — El código que proporciona las funciones de direccionamiento, puenteo, conmutación de enlace de datos y agente de SNMP para el dispositivo.
  - — La interfaz de usuario del direccionador, que permite configurar, supervisar y utilizar el código base de Access Integration Services instalado en el dispositivo. A la interfaz de usuario del direccionador se accede localmente por medio de un terminal o un emulador ASCII conectado a un puerto de servicio, o bien remotamente por medio de una sesión Telnet o de un dispositivo conectado por módem.

  El 2212 lleva el código base instalado de fábrica.
- El Programa de configuración para IBM Access Integration Services (al que en esta publicación llamamos *Programa de configuración*) es una interfaz gráfica de usuario que le permite configurar el dispositivo desde una estación de trabajo autónoma. El Programa de configuración incluye la comprobación de errores y la información de ayuda en línea.

El Programa de configuración no se precarga en la fábrica; se envía por separado del dispositivo, como parte del pedido de software.

El Programa de configuración para IBM Access Integration Services también se puede obtener en Internet, desde la página de presentación IBM Networking Technical Support. En la publicación *Programa de configuración Guía del usuario para productos multiprotocolo y servicios de acceso,* GC10-3430 (GC30-3830), encontrará la dirección y los directorios del servidor.

Convenios utilizados en este manual

Los convenios que figuran a continuación se utilizan en este manual para mostrar la sintaxis de los mandatos y las respuestas del programa:

1. La forma abreviada de un mandato se subraya, tal como se ve en el ejemplo siguiente:

   `reload`

   En este ejemplo, se puede elegir entre escribir todo el mandato (reload) o sólo la abreviatura del mismo (rel).
2. Las elecciones de palabra clave de un parámetro se indican entre corchetes y se separan mediante la conjunción o. Por ejemplo:

   ```
   mandato [palabra_clave_1 o palabra_clave_2]
   ```

   Elija una de las palabras clave como valor para el parámetro.
3. Si a una opción le siguen tres puntos, indica que debe escribir más datos (por ejemplo, una variable) después de la opción. Por ejemplo:

   `time host ...`

   En este ejemplo, en vez de los puntos, se debe escribir la dirección IP del sistema principal (host), tal como se explica en la descripción del mandato.
4. En la información visualizada como respuesta a un mandato, los valores por omisión de una opción se indican entre corchetes inmediatamente después de la opción. Por ejemplo:

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

   En este ejemplo, el medio de transmisión por omisión es UTP, a menos que usted especifique STP.
5. Las combinaciones de teclas del teclado se indican como texto de la siguiente manera:
   - **Control-P**
   - **Control -**

   La combinación de teclas **Control -** indica que debe pulsar simultáneamente la tecla Control y la de guión. En algunas circunstancias, esta combinación de teclas hace que cambie el indicador de línea de mandatos.
6. Los nombres de las teclas del teclado se indican así: **Intro**
7. Las variables (es decir, los nombres utilizados para representar los datos que se definen) se indican en letra cursiva. Por ejemplo:

   `Nombre de archivo: nombrearchivo.ext`

Visión general de la biblioteca

Actualizaciones y correcciones de información: Para mantenerle informado acerca de los cambios técnicos, las aclaraciones y los arreglos que se implementaron una

vez impresas las publicaciones, le remitimos a las páginas de presentación de IBM 2212, en:

`http://www.networking.ibm.com/2212/2212prod.html`

La lista que hay a continuación muestra las publicaciones de la biblioteca de IBM 2212, organizadas según las tareas.

Planificación

GA27-4215 *IBM 2212 Introduction and Planning Guide*

Esta publicación se envía junto con el IBM 2212. En ella se explica cómo prepararse para la instalación y llevar a cabo una configuración inicial.

Instalación

GA27-4216 *IBM 2212 Access Utility Installation and Initial Configuration Guide*

Este librito se envía junto con el IBM 2212. En él se explica cómo instalar el IBM 2212 y verificar la instalación del mismo.

GX27-4048 *2212 Hardware Configuration Quick Reference*

Esta tarjeta de referencia permite entrar y guardar información de configuración de hardware, que se utiliza para determinar el estado correcto de un IBM 2212.

Diagnósticos y mantenimiento

GY27-0362 *IBM 2212 Access Utility Service and Maintenance Manual*

Esta publicación se envía junto con el IBM 2212. En ella se proporcionan instrucciones para el diagnóstico de problemas que puedan surgir en el IBM 2212 y para la reparación del mismo.

Operaciones y gestión de red

La lista que hay a continuación muestra las publicaciones que dan soporte al programa Access Integration Services.

SC10-3436 (SC30-3988)
Software Guía del usuario

En esta publicación se explica cómo:

- Configurar, supervisar y utilizar el software de Access Integration Services.
- Utilizar la interfaz de usuario de direccionador de línea de mandatos de Access Integration Services para configurar y supervisar las interfaces de red y los protocolos de la capa de enlace que se envían junto con IBM 2212.

SC10-3437 (SC30-3989)
Utilización y configuración de características

SC10-3438 (SC30-3990)
Configuración y supervisión de protocolos - Manual de consulta Volumen 1

SC10-3439 (SC30-3991)
Configuración y supervisión de protocolos - Manual de consulta Volumen 2

Resumen de los cambios

En estas publicaciones se describe cómo acceder y utilizar la interfaz de usuario de línea de mandatos de Access Integration Services para configurar y supervisar el software de protocolo de direccionamiento enviado junto con el producto.

En ellas se incluye información acerca de cada uno de los protocolos soportados por los dispositivos.

SC10-3431 (SC30-3682)
Guía de mensajes del sistema para anotaciones de sucesos

Esta publicación contiene un listado de códigos de los errores que pueden producirse, además de las descripciones y acciones recomendadas para corregir los errores.

Configuración

GC10-3430 (GC30-3830)
Programa de configuración Guía del usuario para productos multiprotocolo y servicios de acceso

Esta publicación trata sobre cómo utilizar el programa de configuración.

Seguridad

SD21-0030 *Precaución: Información de seguridad — Lea esto primero*

Esta publicación, que viene con el IBM 2212, proporciona la traducción de los avisos de precaución y peligro aplicables a la instalación y al mantenimiento del IBM 2212.

Márketing

URL: **http://www.networking.ibm.com/2212/2212prod.html**

Esta página Web de IBM proporciona información sobre el producto a través de la World Wide Web.

Resumen de los cambios correspondientes a la biblioteca software IBM 2212

En la siguiente lista figuran los cambios realizados en el software, en la versión 3.3. Los cambios constan de:

- **Funciones nuevas:**
  - — Subsistema de codificación (ES)
  - — Servicios de protocolo de configuración dinámica de sistema principal (DHCP)
  - — Red privada virtual (VPN)
    - – Servicios de directorio: soporte para el protocolo de acceso de directorio ligero (Lightweight Directory Access Protocol) (LDAP)
    - – Soporte para ISAKMP/Oakley
    - – Reenvío de capa 2 (Layer 2 Forwarding) (L2F)
    - – Protocolo de tunelización punto a punto (Point to Point Tunneling protocol) (PPTP)
    - – Servicios diferenciados
  - — Soporte de J2 6 Mbps para máximo de Frame Relay CIR, Bc y Be
  - — Voz a través de Frame Relay

— Fragmentación de paquetes de Frame Relay
— Reenvío de paquetes de voz a través de Frame Relay
— Soporte de WAN profundo
— Señalización RDSI para el adaptador de módem digital

- **Funciones mejoradas:**
  — Mejoras de IP
    – Política de direccionamiento IPv4 genérico
    – Filtros de paquete IPv6, reconfiguración dinámica y soporte de agente de retransmisión DHCP
  — Mejoras de SDLC
    – Sondeo de grupo primario
    – Comunicación simultánea bidireccional
  — Parámetros de configuración de DLSw para permitir el control del número de mensajes de no sesión puestos en cola en el direccionador
  — Mejoras de rendimiento para la función Thin Server
  — Mejoras de TN3270
    – Antememoria de cliente a petición en sistema principal eNetwork de IBM
    – Definición de LU dinámica iniciada por sistema principal
    – Múltiples SA de PU a través de DLSw
  — Mejora en los puentes
    – Soporte de SR-TB para IPX
  — Soporte de reconfiguración dinámica para X.25
  — Mejoras de IPX
    – Ciclos (ticks) de RIP configurables
    – Circuitos SVC de IPXWAN a través de Frame Relay
  — Función de realización de mandato de la interfaz de línea de mandatos
  — Soporte de antememoria de servidor Web en la tarjeta de sistema de alto rendimiento (High Performance System Card), incluyendo las mejoras del gestor de antememoria externa y la alta disponibilidad y escalabilidad
- **Aclaraciones y correcciones**

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

Obtención de ayuda

En los indicadores de mandato, puede obtener ayuda en forma de listado en el que figuren los mandatos que están disponibles a ese nivel. Para ello, escriba **?** (el mandato de **ayuda**) y luego pulse **Intro**. Utilice **?** para listar los mandatos que están disponibles desde el nivel actual. En general, puede entrar **?** después del nombre de un mandato específico para así listar las opciones de ese mandato.

Salida de un entorno de nivel inferior

La naturaleza multinivel del software le va llevando a entornos de nivel secundario, terciario, e incluso inferiores, a medida que configura u opera con el 2212. Para regresar al siguiente nivel superior, entre el mandato **exit**. Para ir al nivel secundario, siga entrando **exit** hasta que reciba el indicador de nivel secundario (ya sea `Config>` o +).

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

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

Si necesita ir al nivel primario (OPCON), entre el carácter de interceptación (que, por omisión, es **Control-P**).

Capítulo 1. Utilización de la reserva de ancho de banda y de colas de prioridad

En este capítulo se describen las características del sistema de reserva de ancho de banda y de las colas de prioridad disponibles actualmente para las interfaces Frame Relay y PPP. Consta de los apartados siguientes:

- "Sistema de reserva de ancho de banda"
- "Reserva de ancho de banda sobre Frame Relay" en la página 3
- "Colas de prioridad" en la página 5
- "BRS y filtros" en la página 7
- "Configuraciones de ejemplo" en la página 12

Sistema de reserva de ancho de banda

El sistema de reserva de ancho de banda (BRS, Bandwidth Reservation System) le permite decidir qué paquetes descartar cuando la demanda (tráfico) en una conexión de red es mayor que la oferta (rendimiento). Cuando la utilización del ancho de banda alcanza el 100%, BRS determina qué tráfico debe descartarse, dependiendo de la configuración.

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

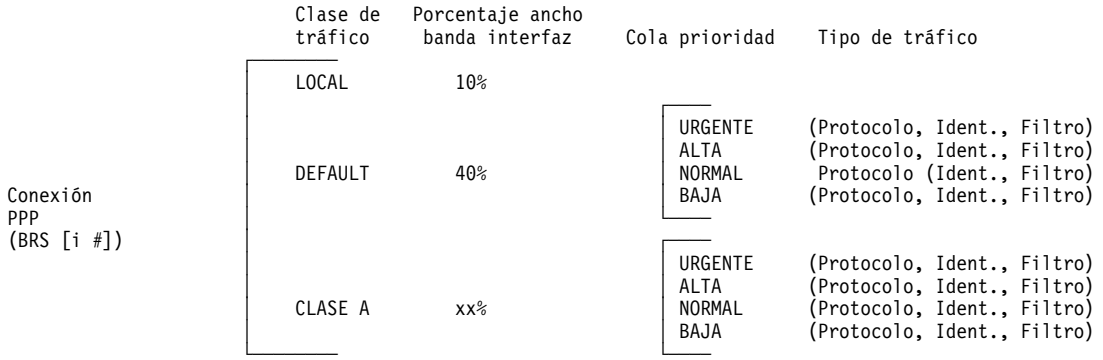
Para las interfaces PPP, se definen clases de tráfico (clases-t) y a cada una se le asigna un porcentaje del ancho de banda de la interfaz PPP. Existen al menos dos clases de tráfico:

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

Se pueden crear clases de tráfico adicionales y asignar protocolos, filtros e identificadores a las colas de prioridad de una clase de tráfico. Consulte la Figura 1 en la página 2.

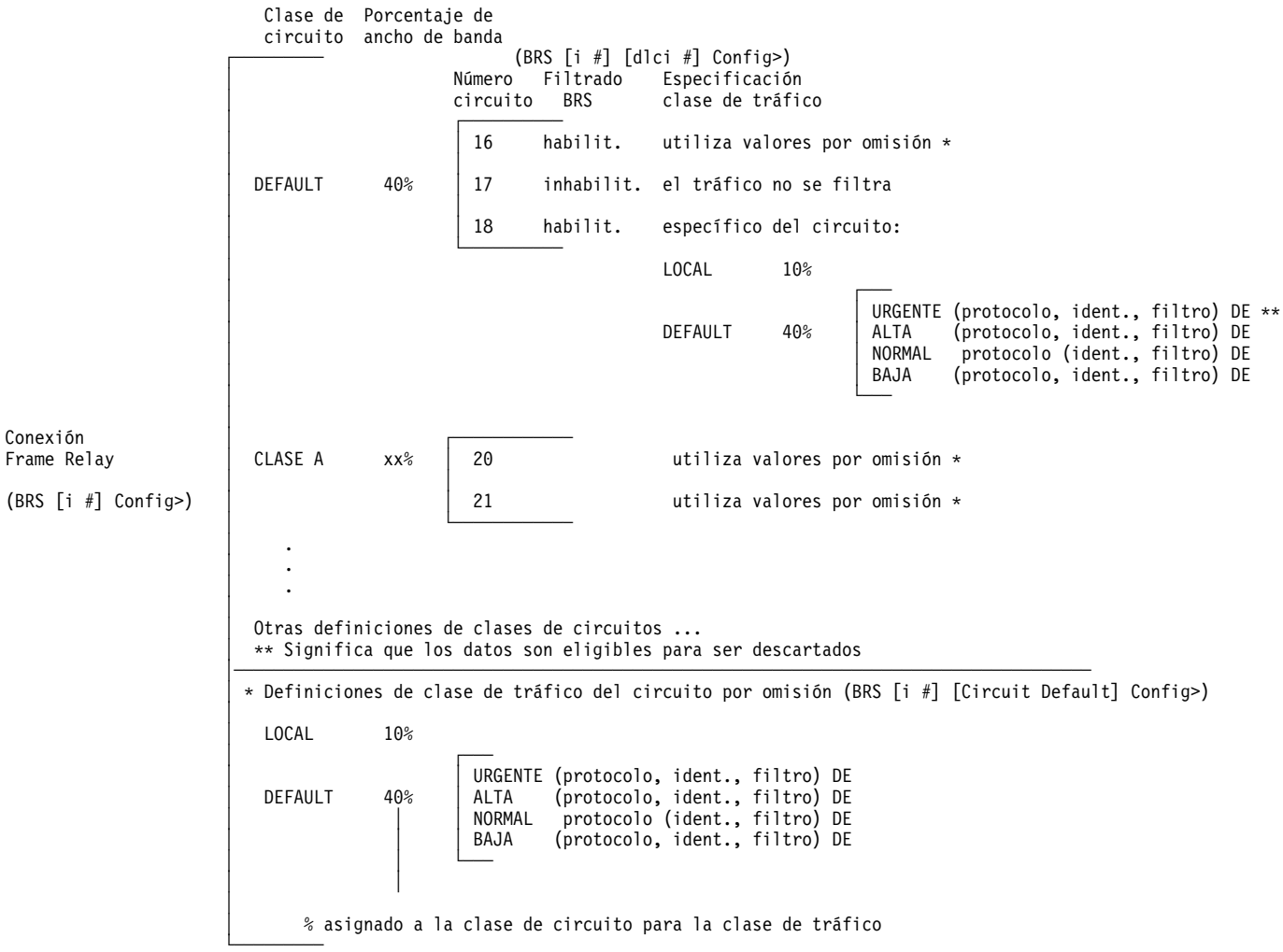
Para las interfaces Frame Relay, se definen clases de circuito (clases-c) y a cada una se le asigna un porcentaje del ancho de banda de la interfaz Frame Relay. Existe al menos una clase de circuito: la clase de circuito DEFAULT, a la que inicialmente se asignan todos los circuitos. Se pueden crear clases de circuito adicionales y asignar circuitos a estas clases-c. Para cada circuito Frame Relay se pueden 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. Los circuitos Frame Relay dan soporte a las clases de tráfico de manera análoga a las interfaces PPP. En la Figura 2 en la página 2 se puede ver la relación entre las clases de circuito y las clases de tráfico Frame Relay.

Utilización de BRS y colas de prioridad



Nota: Inicialmente, a todos los protocolos se les asigna la cola de prioridad NORMAL de la clase de tráfico DEFAULT. Se puede asignar un protocolo, un filtro o un identificador a cualquier cola de una clase de tráfico.

Figura 1. Relación entre la clase de tráfico y la cola de prioridad de la clase de tráfico para una interfaz PPP en BRS



Nota: Inicialmente, a todos los protocolos se les asigna la cola de prioridad NORMAL de la clase de tráfico DEFAULT. Se puede asignar un protocolo, un filtro o un identificador a cualquier cola de una clase de tráfico.

Figura 2. Relación entre la clase de circuito y la clase de tráfico para una interfaz Frame Relay en BRS

Los porcentajes que se reservan son una mínima *parte* del ancho de banda para la conexión de red. Si una red está funcionando al máximo de su capacidad, los mensajes de cada clase sólo podrán transmitirse mientras utilicen el ancho de banda asignado a la clase. En este caso, las transmisiones adicionales se retendrán hasta que se hayan satisfecho otras transmisiones que ocupan ancho de banda. En el caso de que exista una ruta de tráfico poco cargada, una corriente de paquetes podrá utilizar un ancho de banda mayor que el mínimo asignado, llegando al 100% en caso de que no haya más tráfico.

En realidad, la reserva de ancho de banda es un sistema de *salvaguardia.* En general, un dispositivo no debe intentar utilizar más del 100% de la velocidad de la línea. Si lo hace, posiblemente es que se necesita una línea más rápida. Sin embargo, la naturaleza "fluctuante" del tráfico, puede hacer que la velocidad de transmisión supere el 100% durante un corto intervalo de tiempo. En estos casos, se habilita la reserva de ancho de banda y se garantiza la entrega del tráfico de mayor prioridad (es decir, no se descarta).

La reserva de ancho de banda funciona con los tipos de conexión siguientes:

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

Reserva de ancho de banda sobre Frame Relay

La reserva de ancho de banda le permite reservar ancho de banda en los dos niveles siguientes:

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

Cuando BRS recibe un paquete de Frame Relay, se utilizan las clases-c y las clases-t configuradas para determinar cuándo se transmitirá el mismo. BRS pone el paquete en cola de acuerdo a 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 éstas se clasifican según un algoritmo justo ponderado de puesta en cola. En una clase-c, los circuitos que tienen paquetes que transmitir se envían utilizando un algoritmo rotativo. Las clases-t de cada clase-c también se clasifican según un algoritmo justo ponderado de puesta en cola. A su vez, los paquetes de la clase-t se ponen en cola según su prioridad (urgente, alta, normal o baja).

Un paquete se saca de la cola y se transmite cuando cumple todas estas condiciones:

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

Si se habilita la interfaz y uno o más circuitos de BRS, y no se configuran clases-c ni clases-t, todos los circuitos se asignarán a una clase-c llamada *default (por omisión).* Con esta configuración, sólo existirá la clase-c por omisión en la cola de clases-c, y cada uno de los circuitos de la clase-c con paquetes que transmitir se manejará según una estrategia rotativa. Si quiere que BRS haga esto, deje todos los circuitos en la clase-c por omisión y no cree ninguna clase de circuito.

Utilización de BRS y colas de prioridad

Los circuitos huérfanos (no asignados a ninguna clase) y los circuitos para los que no se ha habilitado explícitamente el sistema BRS, utilizarán por omisión este entorno de puesta en cola de BRS en cualquier situación. BRS los asigna a la clase-c por omisión.

Para configurar BRS, debe seguir la secuencia siguiente:

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

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

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

Consulte el Capítulo 2, “Configuración y supervisión de la reserva de ancho de banda” en la página 25, para obtener más información sobre cómo supervisar BRS.

La interfaz es la que se muestra en el indicador de los mandatos de supervisión del ancho de banda. Por ejemplo, `BRS [i 5]` es el indicador de la interfaz 5.

Soporte de colas

Con la reserva de ancho de banda sobre Frame Relay, cada circuito puede poner en cola tramas cuando está congestionado. Esto es válido incluso para interfaces y circuitos para los que no está habilitada la reserva de ancho de banda.

Elegibilidad para ser descartado

La red Frame Relay puede descartar los datos transmitidos que sobrepasen la CIR de un PVC. El direccionador puede poner en 1 el bit DE para indicar que parte del tráfico se debe considerar elegible para ser descartado. En caso necesario, la red Frame Relay descartará las tramas marcadas como elegibles para ser descartadas, lo que permitirá que las tramas que no están marcadas como elegibles para ser descartadas sean transmitidas por la red. Al asignar un protocolo, filtro o identificador a una clase de tráfico, se puede especificar si el tráfico del protocolo, del filtro o del identificador será elegible para ser descartado. En el apartado “Assign” en la página 33 hallará más información sobre cómo configurar el tráfico para que sea elegible para ser descartado. El tráfico de voz (identificado por el protocolo VOFR) debe configurarse como **no** elegible para ser descartado.

Definiciones de circuito por omisión para manejar clases de tráfico

Se pueden definir muchos circuitos para una interfaz Frame Relay. En lugar de tener que configurar totalmente las definiciones de las clases de tráfico de cada circuito, BRS le permite definir un conjunto de clases de tráfico y de asignaciones de protocolos, filtros e identificadores por omisión, llamado definiciones de circuito por omisión, que puede utilizar cualquier circuito de la interfaz. Al habilitar inicialmente BRS para un circuito, éste se inicializa utilizando las definiciones de circuito por omisión. Si un circuito no puede utilizar las definiciones de circuito por omisión para manejar clases de tráfico, se pueden crear definiciones específicas

de circuito mediante los mandatos **add-class**, **change-class**, **assign**, **deassign**, **tag** y **untag**.

Si un circuito utiliza definiciones específicas de circuito y a usted le interesa que utilice 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 manejar clases de tráfico se definen ejecutando el mandato **set-circuit-defaults** en el indicador de la interfaz Frame Relay de BRS. Este mandato le sitúa en un indicador de valores por omisión de circuitos BRS, en el que puede añadir, cambiar y suprimir clases de tráfico, asignar y desasignar protocolos, filtros e identificadores, y crear identificadores de BRS. Si se cambian las definiciones de circuito por omisión para las clases de tráfico, el manejo de las clases de tráfico se actualizará dinámicamente para todos los circuitos que utilicen las definiciones de circuito por omisión.

Configuración de BRS para voz a través de Frame Relay

Las tramas de voz pueden transmitirse por circuitos dedicados. En este caso, habilite BRS para la interfaz y los circuitos, y acepte los valores por omisión de los circuitos asociados con voz. Es posible que quiera crear varias clases-c y asignar los circuitos dedicados a voz a una clase-c asociada con un porcentaje alto de ancho de banda y asignar los circuitos asociados con datos a una clase de circuito asociada con un porcentaje menor de ancho de banda.

Si tanto el tráfico de voz como el resto de tráfico se transmiten por los mismos circuitos, habilite BRS para la interfaz y los circuitos. Si quiere que se atienda a todos los circuitos de forma rotativa, sin favorecer a ningún circuito en particular, puede decidir no crear más clases-c que clase-c por omisión ya existente. A continuación, es recomendable que para cada circuito por el que se transmita voz y datos, cree una clase-t con el mandato **create-super-class** y que asigne el tráfico VOFR a esta clase. Cree también tantas clases-t adicionales como necesite y asigne otros tipos de tráfico a estas clases-t. Esta configuración ayudará a garantizar que el tráfico de voz tenga prioridad sobre el resto de tráfico y que se pueden intercalar tramas de voz sin segmentar entre segmentos de datos fragmentados, si se habilita la fragmentación. Es recomendable que habilite la fragmentación para la interfaz Frame Relay, si quiere enviar voz y datos por la misma interfaz. La fragmentación conlleva que las tramas sean más pequeñas y, de esta forma, que el retardo entre tramas de voz consecutivas también sea menor.

Consulte el mandato **enable fragmentation** en el capítulo “Configuración y supervisión de la interfaz Frame Relay” de la publicación *Software de Access Integration Services Guía del usuario* para obtener más información sobre cómo habilitar la fragmentación.

Colas de prioridad

La reserva de ancho de banda asigna porcentajes del ancho de banda de conexión total para las *clases* de tráfico o *clases-t* especificadas, definidas por el usuario. Exceptuando la clase-t creada con el mandato **create-super-class**, que tiene prioridad sobre las otras clases-t, las clases-t de BRS están asociadas con un porcentaje del ancho de banda. Los datos de protocolos y de filtros pueden asignarse a clases-t y a colas de prioridad concretas de una clase-t. Al utilizar colas de prioridad, puede asignarse un protocolo o un filtro a una cola determinada de una clase de tráfico con valores: una clase-t de BRS es un grupo de paquetes

identificados por el mismo nombre; por ejemplo, una clase llamada “ipx” denomina a todos los paquetes IPX.

Al utilizar colas de prioridad, se puede asignar a cada clase-t de ancho de banda los niveles de prioridad siguientes:

- Urgente
- Alta
- Normal (el valor por omisión)
- Baja

para las clases de tráfico (o clases-t) especificadas, definidas por el usuario.

Además, para cada nivel de prioridad de cada clase-t de ancho de banda, se puede definir el número de paquetes que están esperando en la cola. El mandato **queue-length** de BRS establece el número máximo de almacenamientos intermedios de salida que pueden ponerse en cada cola de prioridad de BRS, y el número máximo de almacenamientos intermedios de salida que pueden ponerse en cada cola de prioridad de BRS cuando escasean los almacenamientos intermedios de entrada del direccionador. Se puede configurar la longitud de las colas de prioridad tanto para PPP como para Frame Relay.

Attention: Si define una longitud de cola demasiado grande, es posible que el rendimiento del direccionador se degrade mucho.

Para BRS, se pueden establecer las longitudes de las colas de prioridad para conexiones WAN PPP y Frame Relay. En el apartado “Queue-length” en la página 47 hallará una descripción del mandato **queue-length**.

Los valores de prioridad de una clase-t de ancho de banda no afectarán a las otras clases de ancho de banda. Ninguna clase de ancho de banda tiene prioridad sobre las otras.

Colas de prioridad sin reserva de ancho de banda

Si las colas de prioridad se configuran sin reserva de ancho de banda, el tráfico que tenga mayor prioridad se entregará primero. En caso de que exista gran cantidad de tráfico con prioridad alta, el tráfico que tenga niveles de prioridad bajos puede quedar totalmente bloqueado. Sin embargo, combinando las colas de prioridades con la reserva de ancho de banda, la transmisión de paquetes puede asignarse a todos los tipos de tráfico.

Configuración de las clases de tráfico

Se pueden crear clases de tráfico mediante el mandato **add-class** y, a continuación, asignar tipos de tráfico a las clases utilizando el mandato **assign**. El tráfico se asigna a una clase de tráfico basándose en su *tipo de protocolo* o en un filtro que a su vez identifica un tipo concreto de *tráfico de protocolo* (por ejemplo, paquetes IP de SNMP).

Los tipos de protocolos soportadod son:

- IP
- ARP
- DNA
- VINES
- IPX
- OSI
- VOFR

- AP2
- ASRT
- SNA/APPN-ISR
- APPN-HPR
- HPR/IP

Filtros de BRS

Si se utiliza la reserva de ancho de banda, se puede tratar el tráfico de un protocolo concreto de forma distinta al de otro tráfico que utilice el mismo tipo de protocolo. Por ejemplo, se puede asignar el tráfico IP de SNMP a una clase de tráfico y prioridad distintas que las del resto de tráfico IP. En este ejemplo, SNMP es un filtro de BRS, ya que *filtra* (o sea, identifica de modo exclusivo) el tráfico de un protocolo concreto. El tráfico de los protocolos IP, ASRT (puentes) y APPN-HPR puede filtrarse mediante la reserva de ancho de banda. Los filtros soportados son los siguientes:

- Túnel IP
- Túnel SDLC a través de IP (retransmisión SDLC)
- Túnel BSC a través de IP (retransmisión BSC)
- Rlogin
- Telnet
- SNA/APPN-ISR
- APPN-HPR
- SNMP
- Multidifusión IP
- DLSw
- Filtro MAC
- NetBIOS
- HPR de red
- HPR alto
- HPR medio
- HPR bajo
- XTP
- Números de puerto o sockets TCP/UDP
- Byte TOS
- bit de precedencia

BRS y filtros

En los apartados siguientes se describe cómo utilizar BRS con distintos tipos de filtros.

Filtrado de direcciones MAC e identificadores

La reserva de ancho de banda y el filtrado MAC (MCF) manejan conjuntamente el filtrado de direcciones MAC utilizando *identificadores*. Por ejemplo, un usuario con reserva de ancho de banda puede categorizar el tráfico que se transmite por un puente asignándole un identificador.

El proceso de identificación consiste en crear un elemento filtro en la consola de configuración del filtrado MAC y asignarle un número de identificador. Este número de identificador se utiliza para configurar una clase de tráfico para todos los paquetes asociados con este identificador. El valor de un identificador debe estar comprendido entre 1 y 64. Consulte el Capítulo 3, “Utilización del filtrado MAC” en la página 55 para obtener información adicional sobre el filtrado MAC.

Utilización de BRS y colas de prioridad

Nota: Los identificadores conciernen ***solamente*** a los paquetes que se transmiten por puentes. En una conexión PPP o Frame Relay, se pueden asignar como filtros de reserva de ancho de banda hasta cinco filtros MAC con identificador, llamados TAG1 a TAG5. En primer lugar se busca TAG1, después TAG2, y así sucesivamente hasta llegar a TAG5. El identificador de un filtro MAC consta de varias direcciones MAC definidas en MCF.

Una vez creado un filtro con identificador en el proceso de configuración de filtrado MAC, podrá utilizar el mandato de configuración de identificadores de BRS para asignar un nombre de identificador de BRS (TAG1, TAG2, TAG3, TAG4 o TAG5) al número de identificador del filtro MAC. A continuación, utilice el nombre de identificador de BRS en el mandato assign de BRS para asignar el filtro MAC correspondiente a la clase de tráfico y prioridad del ancho de banda.

Los identificadores también pueden hacer referencia a "grupos," como en el ejemplo del Túnel IP. Los extremos de un Túnel IP pueden pertenecer a un número indeterminado de grupos. Los paquetes se asignan a un grupo determinado mediante la función de identificación del filtrado de direcciones MAC. Para obtener información adicional sobre el filtrado MAC, consulte el Capítulo 3, "Utilización del filtrado MAC" en la página 55 y el Capítulo 4, "Configuración y supervisión del filtrado MAC" en la página 59.

Para aplicar la reserva de ancho de banda y las colas de prioridad a los paquetes con identificador:

1. Utilice los mandatos de configuración de filtrado MAC desde el indicador `filter config>` para configurar los identificadores de paquetes que se transmiten por el puente. Consulte el Capítulo 3, "Utilización del filtrado MAC" en la página 55 para obtener más información.
2. Utilice el mandato **tag** de la reserva de ancho de banda para referirse a un identificador de reserva de ancho de banda.
3. Con el mandato **assign** de la reserva de ancho de banda, asigne el identificador de BRS a una clase-t. El mandato **assign** también le solicitará que especifique una prioridad de cola para esta clase-t de BRS.

Filtrado de número de puerto TCP/UDP

Se pueden asignar paquetes TCP/IP de un rango de puertos TCP o UDP a una clase-t y prioridad de BRS basándose en el número de puerto UDP o TCP de los paquetes y, opcionalmente, del socket. Se pueden especificar hasta 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 socket (combinación de número de puerto y dirección IP). Después se puede asignar este filtro a una clase de tráfico y prioridad de BRS dentro de la clase.

Si se habilita el filtrado de puertos UDP/TCP, BRS examinará cada paquete TCP o UDP y comprobará si el número de puerto destino u origen coincide con uno de los números de puerto a filtrar. Además, si se define una dirección IP como parte del filtro UDP/TCP de BRS, y la dirección IP destino u origen coincide con la dirección definida para el filtro, BRS asigna el paquete a la clase de tráfico y prioridad de este filtro de número de puerto.

Por ejemplo, se puede configurar un filtro de número de puerto UDP para los números de puerto UDP que van del 25 al 29, y asignar el filtro a la clase de tráfico 'A' con prioridad 'normal'. BRS pone en cola los paquetes UDP cuyo

número de puerto origen o destino va del 25 al 29 en la cola de prioridad normal para la clase de tráfico 'A'.

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

Filtrado de bits TOS de IPv4

Se pueden crear filtros que distingan entre distintos tipos de tráfico IP según el valor de los bits del Tipo de servicio (TOS). Dichos filtros TOS pueden utilizarse para asignar el tráfico IPv4 que tenga determinados valores para los bits TOS a clases y prioridades diferentes de las del tráfico IP. Cada filtro permite el tráfico IPv4 cuyo valor del byte TOS coincide con la definición de un filtro TOS configurado para que se asigne a una clase de tráfico y prioridad exclusivas. Configurar un filtro TOS consiste en especificar un valor de máscara que sirve para definir qué bits del byte TOS deben compararse, así como especificar los valores superior e inferior de los bits que forman parte de la máscara. El mecanismo de filtrado se basa únicamente en los valores del TOS de IPv4; por lo tanto, no se basa en la identificación del tipo de protocolo IPv4 ni en la información del número de puerto, como hacen la mayoría de filtros IP.

La aplicación de este filtro es más ampliable que el método de filtrado de precedencia IPv4 de BRS, que sólo tiene en cuenta los 3 bits situados más a la izquierda del byte TOS. El soporte de filtros de bits TOS de BRS, combinado con el soporte de control de acceso de IP, permite filtrar el tráfico que se envía por un túnel seguro, que esté fragmentado o que no pueda identificarse mediante el soporte de filtros de número de puerto UDP o TCP de BRS. Además, el soporte de control de acceso de IP permite establecer los bits TOS en valores definidos por el usuario, en lugar de tener que utilizar los valores de los bits de precedencia para APPN y DLSw, que no pueden modificarse, asociados con el filtrado de bits de precedencia IPv4 de BRS. Por lo tanto, es recomendable que utilice el soporte de control de acceso de IP y de filtros de bits TOS, en lugar del método de filtrado de bits de precedencia IPv4 de BRS.

Como se indica en el apartado "Orden de precedencia del filtrado" en la página 12, la comprobación de las coincidencias con los filtros TOS se realiza antes que la de los filtros de bits de precedencia IPv4 y que la de otros filtros específicos de IP. La comprobación de las coincidencias con los filtros TOS1 a TOS5 se hace secuencialmente, empezando por el filtro TOS1. Pueden definirse hasta 5 filtros TOS.

Importante: Tenga presente que un paquete con un determinado valor del TOS, se manejará según sea la primera definición de los filtros TOS con que coincida el valor. Los filtros deben configurarse cuidadosamente para que un determinado byte TOS se filtre por el filtro correspondiente y no, accidentalmente, por un filtro anterior. En el apartado "Utilización de IP", de la publicación *Utilización y configuración de características*, hallará más información.

Proceso de bits de precedencia de IP versión 4 para tráfico SNA en túneles seguros IP y fragmentos secundarios

Normalmente, BRS distingue entre el tráfico TCP de IP y el tráfico UDP de IP según sus números de puerto. Sin embargo, BRS no puede identificar los puertos después de que el tráfico se haya encapsulado dos veces, como es el caso del tráfico IP transmitido a través de un túnel seguro o en un fragmento UDP o TCP secundario. El proceso de bits de precedencia de IP versión 4 se ha añadido a BRS para permitirle filtrar los paquetes transmitidos a través de un túnel seguro IP y en fragmentos secundarios de TCP y UDP.

Nota: Es recomendable que utilice el método de filtrado de bits TOS de IPv4 de BRS en lugar del proceso de bits de precedencia IPv4. Para obtener más detalles, consulte el apartado “Filtrado de bits TOS de IPv4” en la página 9.

Cuando el tráfico APPN/HPR se direcciona a través de IP, las prioridades de la transmisión de APPN-HPR (de red, alta, media y baja), se correlacionan con un valor particular de los tres bits de precedencia de IP versión 4.

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

Si se habilita el filtrado de precedencia IPv4 para BRS y los bits de precedencia de un paquete IP coinciden con uno de los valores utilizados por el tráfico APPN/HPR, el paquete se pondrá en la cola de prioridad de la clase-t de BRS a la que esté asignada la correspondiente prioridad de transmisión de HPR. Por ejemplo, si un paquete IP tiene un valor de precedencia '110'b y el filtro HPR de red de BRS está asignado a una clase-t A con un nivel de prioridad normal, el paquete se pondrá en la cola de prioridad normal de la clase-t A. Si no se ha configurado ningún filtro de prioridad de la transmisión de HPR de BRS, el paquete se pondrá en la cola de prioridad de la clase-t a la que esté asignado el filtro APPN-HPR.

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

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

Al correlacionar distintos tipos de tráfico con un solo valor, BRS no puede distinguirlos cuando se habilita el filtrado basado en los bits de precedencia IPv4. Por lo tanto, cuando BRS se encuentra un paquete IP con un valor de precedencia '011'b, evalúa los filtros de BRS en el orden siguiente para determinar si el filtro está habilitado o no. Si encuentra un filtro de BRS configurado, el paquete se pone en la cola de prioridad de clase-t a la que está asignado el filtro de BRS:

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

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

Si un cliente envía tráfico TN3270 al 2212 a través de una red de área amplia en la que está habilitado BRS, éste no podrá asignar prioridades al tráfico del cliente, a menos que el cliente defina los bits de precedencia como '011'b.

El manejo de bits de precedencia IPv4 debe configurarse en varios sitios:

1. En BRS se configura si BRS debe filtrar o no basándose en los bits de precedencia IPv4. Sólo realizará esté tipo de filtrado para paquetes transmitidos por túneles seguros IP y que estén en fragmentos secundarios de TCP y UDP.
2. Al configurar DLSw, HPR sobre IP y TN3270, se especifica si el 2212 debe o no debe establecer los bits de precedencia IPv4 para los paquetes que cree para cada uno de estos tipos de protocolo.

Para utilizar el método de filtrado de bits de precedencia IPv4 siga estos tres pasos:

1. Active el filtrado de precedencia IPv4 en BRS.
2. Configure las clases-t de BRS y asigne protocolos y filtros para tantas categorías de tráfico SNA como quiera, para el tráfico SNA que no se transmita a través de un túnel seguro IP o que no esté fragmentado.
3. Habilite los valores de los bits de precedencia IPv4 al configurar los protocolos DLSw, HPR sobre IP y TN3270.
4. Configure IPsec para crear un túnel seguro por el que se transmitirá el tráfico DLSw, HPR sobre IP e TN3270.

Filtrado de SNA y APPN para tráfico que se transmite por un puente

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

Nota: Los paquetes BAN de Frame Relay entran dentro de esta categoría.

Los filtros APPN-HPR le permiten asignar a una clase-t de BRS el tráfico HPR transmitido por un puente. El tráfico HPR se identifica como los paquetes transmitidos por un puente cuyo SAP origen o destino es 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 HPR de red, HPR alto, HPR medio y HPR bajo permiten que el tráfico HPR transmitido por un puente vuelva a filtrarse dependiendo de la prioridad de transmisión de HPR. Por ejemplo, si quiere asignar el tráfico HPR con prioridad de transmisión de red a una determinada clase-t y prioridad, y el resto de tráfico HPR transmitido por un puente a una clase-t y prioridad diferentes, asigne el filtro HPR de red a la clase-t y prioridad adecuadas y utilice el filtro APPN-HPR para asignar el resto de tráfico HPR a una clase-t o prioridad distintas.

Utilización de BRS y colas de prioridad

El tráfico APPN-HPR que se va a direccionar a través de IP se filtra utilizando el número de puerto UDP asignado para las prioridades de red, alta, media y baja de la transmisión de HPR. Para los intercambios XID se utiliza un número de puerto UDP adicional. Todos los números de puerto UDP utilizados para dar soporte a APPN-HPR sobre IP son configurables.

Si APPN no está habilitado en un direccionador intermedio de la red IP, los números de puerto UDP para HPR sobre IP se pueden configurar 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 pueden ayudarle a asignar el tráfico. Por ejemplo, el filtro DLSw le permite asignar el tráfico SNA-DLSw que se enviará a través de una conexión TCP a una clase-t de BRS

Para los filtros SNA/APPN-ISR y APPN-HPR, si quiere que la comprobación se realice con otros SAP distintos de los anteriores, cree un filtro de ventana corredera utilizando el filtrado MAC e identificando el filtro. A continuación, asigne el filtro MAC con identificador a una clase-t de BRS.

Orden de precedencia del filtrado

Es posible que al comparar un paquete, éste coincida con más de un tipo de filtro de BRS. Por ejemplo, un paquete IP transmitido por un puente y un túnel que contiene datos SNA puede coincidir con el filtro de túnel IP y con el filtro SNA/APPN-ISR. El orden de evaluación de los filtros para determinar si un paquete coincide o no con un tipo de filtro de BRS es el siguiente:

1. Filtros TOS (IP)
2. Manejo de precedencia IPv4
3. Comparación del identificador de un filtro MAC para paquetes transmitidos por puentes (IP/ASRT)
4. NetBIOS para paquetes transmitidos por puentes (IP/ASRT)
5. SNA/APPN-ISR para paquetes transmitidos por puentes (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 números de puerto UDP/TCP (IP)
12. Túnel IP (IP)
13. Retransmisión SDLC/BSC (IP)
14. DLSw (IP)
15. Multidifusión (IP)
16. SNMP (IP)
17. Rlogin (IP)
18. Telnet (IP)
19. XTP (IP)

Nota: Los protocolos relacionados con el filtro aparecen entre paréntesis.

Configuraciones de ejemplo

Uso de las definiciones de circuito por omisión para manejar clases de tráfico de circuitos Frame Relay

Notas:

1 Configura la característica BRS.
2 Habilita la característica BRS para la interfaz 1.
3 Habilita la característica BRS para los circuitos 16, 17, 18. Estos circuitos utilizan las definiciones de circuito por omisión para manejar clases de tráfico.
4 Accede al menú set-circuit-defaults para definir las definiciones de circuito por omisión para manejar clases de tráfico.
5 Añade clases de tráfico y asigna protocolos y filtros a dichas clases de tráfico.
6 Lista y muestra las definiciones de BRS para el circuito 16. Puesto que el circuito 16 utiliza las definiciones de circuito por omisión, se mostrarán las clases de tráfico y las asignaciones de protocolos y filtros definidas por las definiciones de circuito por omisión.
7 Cambia el circuito 17 para que pase de utilizar las definiciones de circuito por omisión a utilizar definiciones de circuito propias para manejar clases de tráfico, creando una clase exclusiva, CIRC171. A esta clase se le pueden asignar protocolos, filtros o identificadores.
8 Cambia las definiciones de circuito por omisión de forma que las clases de tráfico DEF1 y DEF2 reserven cada una el 10% del ancho de banda y, a continuación, se muestra que los cambios se han aplicado al circuito 16, pero no al circuito 17, puesto que éste utiliza ahora definiciones de circuito propias.
▌ Altera el circuito 17 para que utilice las definiciones de circuito por omisión para manejar clases de tráfico en lugar de las definiciones de circuito propias.

Utilización de BRS y colas de 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.
```

```
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
```

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

Utilización de BRS y colas de 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]? CIRC171
 Percent bandwidth to reserve [10]? 5
 BRS[i 1] [dlci 17] Config>assign vines
 Class name [DEFAULT]? CIRC171
 Priority <URGENT/HIGH/NORMAL/LOW> [NORMAL]?
 Frame Relay Discard Eligible <NO/YES>[NO]?
```

```
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
```

```
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] [dlci 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
```

```
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 colas de 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
  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] [dlci 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] [dlci 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
```

Capítulo 2. Configuración y supervisión de la reserva de ancho de banda

En este capítulo se describen los mandatos de configuración y de funcionamiento del sistema de reserva de ancho de banda (BRS).

Este capítulo consta de los apartados siguientes:

- "Visión general de la configuración de la reserva de ancho de banda"
- "Mandatos de configuración de la 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 la reserva de ancho de banda" en la página 50

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 configurarla en el direccionador:

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

   Este es el nivel de indicador de interfaz y en esta instancia el número de interfaz es cero. Para cada interfaz que vaya a configurar, tendrá que repetir los pasos 3 y 4.

   Si está configurando el BRS para una interfaz Frame Relay, continúe en el paso 4a:

   Si está configurando BRS para otra interfaz, vaya directamente al paso 5.

   a. En el indicador `BRS [i 0] Config>`, escriba **circuit** #, donde # es el número del circuito que quiere configurar.
   b. En el indicador `BRS [i 0] [dlci 16] Config>`, escriba **enable**. Este es el nivel de indicador de circuito y en esta instancia el número de circuito (DLCI) es 16.
   c. En el indicador `BRS [i 0] [dlci 16] Config>`, escriba **exit** para volver al nivel de indicador de interfaz.
   d. Repita los pasos 4a a 4c para cada circuito para el que quiera definir clases-t de 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 concreta que acaba de habilitar.
7. Si está configurando BRS para una interfaz PPP, configure las clases de tráfico y asígneles protocolos, filtros e identificadores en el indicador `BRS[i 0]Config>` mediante los mandatos que se listan en la Tabla 3 en la página 29. Si está configurando BRS para una interfaz FR (Frame Relay), continúe con los pasos 8 a 10.
8. Si está configurando BRS para una interfaz FR, puede configurar clases de circuitos y asignarles circuitos mediante los mandatos que se listan en la Tabla 2 en la página 28

9. Si quiere utilizar las definiciones de circuito por omisión, entonces escriba el mandato **set-circuit-defaults** en el indicador `BRS[i 0]Config>`. Esto le lleva al indicador `BRS[i 0][circuit defaults]` en el que podrá utilizar los mandatos adecuados de la Tabla 3 en la página 29 para configurar las clases de tráfico y asignarles protocolos, filtros e identificadores. Una vez haya terminado de definir las definiciones de circuito por omisión para manejar clases de tráfico, escriba "exit" para volver al indicador `BRS[i 0] Config>`.
10. Si tiene circuitos FR que no pueden utilizar las definiciones de circuito por omisión para manejar clases de tráfico, escriba **circuit** *circuito-permanente-virtual número_circuito*. Esto le llevará al indicador de circuito, donde podrá utilizar los mandatos que se listan en la Tabla 3 en la página 29 para crear definiciones de circuito propias para manejar clases de tráfico.

Nota: No es necesario que vuelva a cargar el direccionador para que los cambios hechos en la configuración de las clases-t y de las clases-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 escribir este mandato utilizando el nombre (brs) o el número (1) de la función.

El mandato **interface #** le permite seleccionar la interfaz concreta que se quiere configurar para la reserva de ancho de banda. Antes de configurar las clases de BRS, deberá utilizar el mandato **enable** para habilitar BRS para la interfaz. En el paso 4 en la página 25, el indicador muestra que el número de interfaces seleccionadas es cero.

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

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

Para volver al indicador `Config>` sólo tiene que entrar el mandato **exit** en cada uno de los niveles de indicador de BRS, hasta llegar al indicador `Config>`.

Mandatos de configuración de la reserva de ancho de banda

En este apartado se describen los mandatos de configuración de la reserva de ancho de banda. Los mandatos que pueden utilizarse varían dependiendo del indicador de configuración de BRS que se muestre (`BRS Config>`, `BRS [i x] Config>`, o `BRS [i x] [dlci y] Config>` o `BRS [i x] [circuit defaults] Config>`).

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

Mandato	Función
? (Ayuda)	Visualiza todos los mandatos disponibles para este nivel de mandato, o lista las opciones de mandatos específicos (si es que están disponibles). Consulte “Obtención de ayuda” en la página xxv.
Activate-IP-precedence-filtering	Activa el filtrado de precedencia IPv4 de BRS para paquetes APPN y SNA que se envían por túneles IP seguros o que están en fragmentos TCP o UDP secundarios. También debe configurar el valor de los bits de precedencia IPv4 al configurar DLSw, HPR sobre IP o TN3270.
Deactivate-IP-precedence-filtering	Desactiva el proceso de filtrado de precedencia IPv4.
Enable-hpr-over-ip-port-numbers	Habilita el filtrado de BRS para el tráfico APPN-HPR sobre IP y permite la configuración de los números de puerto UDP utilizados para identificar los paquetes HPR sobre IP. **Nota:** Si APPN está incluido en la imagen de carga, no se da soporte a este mandato puesto que BRS se informa en APPN de si se ha configurado HPR sobre IP y, si es así, BRS se informa en APPN de los números de puerto UDP que utilizarán los paquetes HPR sobre IP.
Disable-hpr-over-ip-port-numbers	Inhabilita el filtrado de BRS del tráfico APPN-HPR sobre IP. **Nota:** Si APPN está incluido en la imagen de carga, no se dará soporte a este mandato puesto que BRS se informa en APPN de si se ha configurado o no HRP sobre IP.
Interface	Selecciona una interfaz para la que configurar la reserva de ancho de banda. **Nota:** Este mandato debe escribirse antes de utilizar cualquier mandato de configuración. Consulte la Tabla 2 en la página 28 y la Tabla 3 en la página 29.

Configuración de BRS y colas de prioridad

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

Mandato	Función
List	Lista las interfaces que dan soporte a la reserva de ancho de banda e indica si la reserva de ancho de banda está habilitada o inhabilitada para cada una de ellas.
Exit	Hace volver al nivel de mandato anterior. Consulte "Salida de un entorno de nivel inferior" en la página xxv.

Tabla 2. Mandatos de configuración de interfaz de BRS disponibles desde el indicador BRS [i #] Config> para interfaces Frame Relay

Mandato	Función
? (Ayuda)	Visualiza todos los mandatos disponibles para este nivel de mandato, o lista las opciones de mandatos específicos (si es que están disponibles). Consulte "Obtención de ayuda" en la página xxv.
Add-circuit-class	Establece el nombre de una clase-c de ancho de banda y su porcentaje de ancho de banda.
Assign-circuit	Asigna un circuito determinado a la clase-c de ancho de banda especificada.
Change-circuit-class	Cambia el ancho de banda configurado para una clase-c de ancho de banda.
Circuit	Accede al indicador de nivel de circuito de BRS (`BRS [i x][dlci y] Config>`) desde el que se pueden utilizar los mandatos que se listan en la Tabla 3 en la página 29 para configurar la reserva de ancho de banda para el circuito Frame Relay.
Clear-block	Borra de la memoria SRAM los datos de configuración asociados con la interfaz actual. Se borran los datos de configuración de la clase de circuito y las definiciones de circuito por omisión para manejar 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 de 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 para la interfaz.
Enable	Habilita la reserva de ancho de banda para la interfaz.
List	Visualiza las clases-c y las definiciones de circuito asignadas, almacenadas en la memoria SRAM.
Queue-length	Establece el número máximo y mínimo de paquetes que puede haber en una cola de prioridad.
Set-circuit-defaults	Accede al indicador de mandatos `BRS [i x] [circuit defaults] Config>` lo que le permitirá utilizar los mandatos de la Tabla 3 en la página 29 para crear las definiciones de circuito por omisión para manejar clases de tráfico.
Show	Visualiza las clases-c definidas y los circuitos asignados actualmente, almacenados en la memoria SRAM.
Exit	Hace volver al nivel de mandato anterior. Consulte "Salida de un entorno de nivel inferior" en la página xxv.

En la tabla siguiente se listan los mandatos de circuito de BRS disponibles desde los indicadores `BRS [i x] Config>` para interfaces PPP, `BRS [i x] dlci [y] Config>` para circuitos Frame Relay y `BRS [i x] [circuit defaults] Config>`.

Tabla 3 (Página 1 de 2). Mandatos para manejar clases de tráfico de BRS

Mandato	Función
? (Ayuda)	Visualiza todos los mandatos disponibles para este nivel de mandato, o lista las opciones de mandatos específicos (si es que están disponibles). Consulte “Obtención de ayuda” en la página xxv.
Add-class	Asigna un determinado ancho de banda a una clase de tráfico definida por el usuario.
Create-super-class	Define la clase-t llamada *super-class*.
Assign	Asigna un protocolo o filtro a una clase de tráfico ya configurada.
Change-class	Cambia el ancho de banda configurado para una clase-t de ancho de banda.
Clear-block	Borra de la memoria SRAM los datos de configuración de la clase de tráfico y de la asignación de protocolos, filtros e identificadores, para la interfaz PPP o el circuito Frame Relay. **Nota:** Este mandato no puede utilizarse desde el indicador `BRS [i x] [circuit defaults] Config>`.
Deassign	Restaura la clase-t y prioridad por omisión a la cola del paquete o filtro especificados.
Default-class	Establece la clase-t y prioridad por omisión a los valores deseados y asigna todos los protocolos que no están asignados a la nueva clase-t por omisión.
Del-class	Suprime una clase-t de ancho de banda ya configurada.
Disable	Inhabilita la reserva de ancho de banda para la interfaz PPP o el circuito Frame Relay. **Nota:** BRS no puede habilitarse ni inhabilitarse desde el indicador `BRS [i x] [circuit defaults] Config>`.
Enable	Habilita la reserva de ancho de banda para la interfaz PPP o el circuito Frame Relay. **Nota:** BRS no puede habilitarse ni inhabilitarse desde el indicador `BRS [i x] [circuit defaults] Config>`.
List	Lista las clases-t y las asignaciones de protocolos, filtros e identificadores configuradas, almacenadas en la memoria SRAM.
Queue-length	Establece el número máximo y mínimo de paquetes que puede haber en una cola de prioridad. **Nota:** Este mandato no puede utilizarse desde el indicador `BRS [i x] [circuit defaults] Config>`.
Show	Visualiza las clases-t y las asignaciones de protocolos, filtros e identificadores definidas actualmente, almacenadas en la memoria SRAM. **Nota:** Este mandato no puede utilizarse desde el indicador `BRS [i x] [circuit defaults] Config>`.
Tag	Asigna un nombre de identificador de BRS (TAG1 a TAG5) a un filtro MAC al que se ha asignado un identificador durante la configuración de la función de filtrado MAC.

Tabla 3 (Página 2 de 2). Mandatos para manejar clases de tráfico de BRS

Mandato	Función
Untag	Elimina la relación entre un nombre de identificador de BRS (TAG1 a TAG5) y un filtro MAC al que se ha asignado un identificador durante la configuración de la función de filtrado MAC.
Use-circuit-defaults	Permite que el usuario suprima las definiciones de circuito propias y utilice las definiciones de circuito por omisión para manejar clases de tráfico. Este mandato es válido en el indicador `BRS [i x] dlci [y] Config>`, sólo para Frame Relay. **Nota**: Para que los valores por omisión sean operativos, se debe volver a cargar el direccionador.
Exit	Hace volver al nivel de mandato anterior. Consulte “Salida de un entorno de nivel inferior” en la página xxv.

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

Notas:

1. Si se ejecutan los mandatos **clear-block**, **disable**, **enable**, **list** o **show** desde el menú de interfaz de BRS, la información de reserva de ancho de banda configurada para la interfaz seleccionada se modificará o se listará. Si los mandatos se ejecutan desde el menú de circuito de BRS, sólo se modificará o se listará la información de reserva de ancho de banda de Frame Relay configurada para el circuito virtual permanente (PVC).
2. Antes de utilizar los mandatos de reserva de ancho de banda, tenga presentes los puntos siguientes:
   - Antes de utilizar cualquier mandato de configuración, debe utilizar el mandato **interface** para seleccionar una interfaz (obligado por la configuración de BRS).
   - El parámetro *nombre-clase* es sensible a las mayúsculas y minúsculas.
   - Para ver los *nombres de clase* actuales, utilice los mandatos **list** o **show**.
   - Después de habilitar la reserva de ancho de banda para una interfaz o para un circuito, podrá añadir, suprimir o cambiar circuitos y clases de tráfico, y asignar circuitos o protocolos dinámicamente. Los únicos mandatos que obligan a volver a cargar el direccionador para que entren en vigor son enable, disable, use-circuit-defaults y clear-block.
3. No es necesario volver a cargar el direccionador para que las modificaciones en la configuración de las clases-t y de las clases-c entren en vigor.

Activate-IP-precedence-filtering

Utilice el mandato **activate-ip-precedence-filtering** para activar el filtrado de precedencia IPv4 de BRS para paquetes APPN y SNA que se envían por un túnel IP seguro o que están en fragmentos TCP o UDP secundarios. También debe configurar el valor de los bits de precedencia IPv4 al configurar DLSw, HPR sobre IP o TN3270. Para obtener más información, consulte el apartado “Proceso de bits de precedencia de IP versión 4 para tráfico SNA en túneles seguros IP y fragmentos secundarios” en la página 10.

Sintaxis:

ac**tivate-ip-precedence-filtering**

Add-circuit-class

Nota: Sólo se utiliza en la configuración de Frame Relay.

Utilice el mandato **add-circuit-class** en el nivel de interfaz para asignar un determinado ancho de banda que utilizará un grupo de circuitos asignados a la clase-c de ancho de banda definida por el usuario.

Sintaxis:

add-ci**rcuit-class** *nombre-clase %*

Add-class

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

Nota: Si el mandato se ejecuta para un circuito Frame Relay que está utilizando actualmente definiciones de circuito por omisión para manejar clases de tráfico, se le preguntará si quiere alterar temporalmente las definiciones de circuito por omisión. Si la respuesta es afirmativa, el circuito se cambiará para que utilice las definiciones de circuito propias para manejar clases de tráfico, y se aceptará el mandato. Si la respuesta es "No", el mandato se cancelará anormalmente y el circuito seguirá utilizando las definiciones de circuito por omisión. Si quiere cambiar las definiciones de circuito por omisión, debe ir al indicador de mandatos `BRS [i x][circuit defaults]Config>`.

Sintaxis:

| add-cl**ass** [*nombre-clase* o *número-clase*] *%*

| **Ejemplo 1: Añadir una clase llamada CIRC17 a 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: Añadir una clase llamada clase1 a un circuito Frame Relay

```
BRS [i 2] [dlci 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] [dlci 128]>add clase1
Percent bandwidth to reserve [10]?
BRS [i 2] [dlci 128]>

BRS [i 2] [dlci 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 clase1 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] [dlci 128]>
```

Assign

Utilice el mandato **assign** para asignar identificadores, paquetes de protocolos o filtros a una clase-t determinada, y asignarle prioridad. Los cuatro tipos de prioridad son:

- Urgente
- Alta
- Normal (prioridad por omisión)
- Baja.

Nota: El protocolo Voz sobre Frame Relay (VOFR) se utiliza para enviar paquetes de voz a través de una interfaz Frame Relay. Si un circuito transportará únicamente paquetes de voz, asigne una sola clase-t al circuito y especifique que el protocolo es VOFR. Sólo se permite una clase-t porque así no tendrá prioridad sobre otras. Si hubiera más de una clase-t, las que no transportaran voz podrían hacerse con el control del ancho de banda e interferir en la transmisión del tráfico de voz. Para garantizar que el tráfico de voz se transmita inmediatamente, debe asignarse el tipo de prioridad *Urgente* al tráfico VOFR y únicamente a este tráfico.

Configuración de BRS y colas de prioridad

Debe configurarse la función de Fragmentación en Frame Relay, descrita en el mandato **enable fragmentation**, en el capítulo “Configuración y supervisión de interfaces Frame Relay”, de la publicación *Software de Access Integration Services Guía del usuario*, en caso de que el tráfico que se vaya a transportar por el circuito sea tanto de datos como de voz. Esto es necesario para evitar que grandes paquetes de datos utilicen todo el ancho de banda, impidiendo que los paquetes de voz se envíen lo suficientemente deprisa.

Sintaxis:

assign	[*clase-protocolo* o IDENTIFICADOR o *clase-filtro*] [*nombre-clase* o *número-clase*]

El mandato **assign** también le permite establecer el bit Elegible para descartar (DE) para las tramas Frame Relay.

Nota: Si el mandato se ejecuta para un circuito Frame Relay que está utilizando actualmente definiciones de circuito por omisión para manejar clases de tráfico, se le preguntará si quiere alterar temporalmente las definiciones de circuito por omisión. Si la respuesta es afirmativa, el circuito se cambiará para que utilice las definiciones de circuito propias para manejar clases de tráfico, y se aceptará el mandato. Si la respuesta es “No”, el mandato se cancelará anormalmente y el circuito seguirá utilizando las definiciones de circuito por omisión. Si quiere cambiar las definiciones de circuito por omisión, debe ir 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: Asignar un filtro TOS a la clase clase1; clase1 se ha añadido previamente a la configuración con el mandato *add class***.**

```
BRS [i 2] [dlci 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]? clase1  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] [dlci 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 clase1 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 clase1 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                 clase1               NORMAL            NO
   with TOS range x1 - x3
    and TOS mask xFF

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

1 Para utilizar el filtro TOS debe entrar tres parámetros: TOS mask, TOS range-low y TOS range-high. Consulte el mandato “Add” en el capítulo “Configuración y supervisión IP”, de la publicación *Configuración y supervisión de protocolos - Manual de consulta Volumen 1*, para obtener una descripción de estos parámetros.

Assign-circuit

Nota: Sólo se utiliza en la configuración de Frame Relay.

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

Nota: Debe utilizar el mandato **circuit** para habilitar BRS para el circuito virtual y, a continuación, debe reiniciar o volver a cargar el direccionador antes de poder utilizar este mandato para asignar el circuito a una clase de circuito.

Sintaxis:

assign-c**ircuit** *número-circuito nombre-clase*

Change-circuit-class

Nota: Sólo se utiliza en la configuración de Frame Relay.

Utilice el mandato **change-circuit-class** en el nivel de interfaz para cambiar el porcentaje de ancho de banda que utilizará el grupo de circuitos asignados a la clase-c especificada.

Sintaxis:

change-ci**rcuit-class**
nombre-clase *%*

Change-class

Utilice el mandato **change-class** para cambiar el ancho de banda configurado para una clase-t de ancho de banda.

Nota: Si el mandato se ejecuta para un circuito Frame Relay que está utilizando actualmente definiciones de circuito por omisión para manejar clases de tráfico, se le preguntará si quiere alterar temporalmente las definiciones de circuito por omisión. Si la respuesta es afirmativa, el circuito se cambiará para que utilice las definiciones de circuito propias para manejar clases de tráfico, y se aceptará el mandato. Si la respuesta es "No", el mandato se cancelará anormalmente y el circuito seguirá utilizando las definiciones de circuito por omisión. Si quiere cambiar las definiciones de circuito por omisión, debe ir al indicador de mandatos `BRS [i x][circuit defaults]Config>`.

Sintaxis:

change-cl**ass** [*nombre-clase* o *número-clase*] *%*

Circuit

Nota: Sólo se utiliza en la configuración de 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 ejecutarse desde el indicador de configuración de interfaz de BRS (`BRS [i #] Config>`).

Sintaxis:

*ci***rcuit**

Antes de utilizar los mandatos **add-class**, **assign**, **default-class**, **del-class**, **deassign** o **change-class**, deberá habilitar BRS para el circuito y reiniciar o 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 ejecutar el mandato **enable** para el circuito Frame-Relay y de reiniciar o volver a cargar el direccionador, los mandatos siguientes 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 memoria SRAM los datos de la configuración actual de la reserva de ancho de banda.

Sintaxis:

c**lear-block**

- Si escribe el mandato en el indicador de interfaz para PPP, se borrarán todos los datos de configuración de BRS para la interfaz.
- Si escribe el mandato en el indicador de interfaz para Frame Relay, BRS ya no estará habilitado para la interfaz ni para los circuitos de la interfaz y, además, se borrarán todos los datos de configuración de las clases de circuito y las definiciones de circuito por omisión para manejar clases de tráfico. Sin embargo, no se borrarán los datos de configuración de las clases de tráfico de cada circuito individual y estarán disponibles si se vuelve a habilitar BRS para la interfaz.
- Para borrar los datos de configuración de las clases de tráfico de un circuito, primero deberá entrar el mandato **circuit** desde el indicador de nivel de interfaz y, a continuación, el mandato **clear-block** desde el indicador de nivel de circuito. Después de borrar los datos de configuración de las clases de tráfico para todos los circuitos, escriba el mandato **clear-block** desde el indicador de nivel de interfaz para borrar los datos de configuración de las clases de circuito. Los cambios no entrarán en vigor hasta que el direccionador se reinicie o se vuelva 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 llamada *super-class* para la interfaz PPP o el circuito Frame Relay. Sólo se puede configurar una clase super-class para cada interfaz PPP o circuito Frame Relay. No se asocia ningún porcentaje de ancho de banda a la clase super-class. Los datos de un protocolo o filtro asignados a una clase super-class se transmitirán antes que los datos de un protocolo o filtro asignados a otras clases-t de la interfaz PPP o el circuito Frame Relay. Para el protocolo Voz sobre Frame Relay (VOFR), se debe configurar una clase super-class para un circuito que transporte tanto paquetes de

voz como de datos. En este entorno, si se configura la clase super-class para que transporte voz, es más probable que los paquetes de voz tengan mayor prioridad.

Sintaxis:

cr**eate-super-class**

Deactivate-IP-precedence-filtering

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

Sintaxis:

de**activate-ip-precedence-filtering**

Deassign

Utilice el mandato **deassign** para restaurar la clase-t y prioridad por omisión de la cola del paquete de un protocolo o filtro especificados.

Nota: Si el mandato se ejecuta para un circuito Frame Relay que está utilizando actualmente definiciones de circuito por omisión para manejar clases de tráfico, se le preguntará si quiere alterar temporalmente las definiciones de circuito por omisión. Si la respuesta es afirmativa, el circuito se cambiará para que utilice las definiciones de circuito propias para manejar clases de tráfico, y se aceptará el mandato. Si la respuesta es "No", el mandato se cancelará anormalmente y el circuito seguirá utilizando las definiciones de circuito por omisión. Si quiere cambiar las definiciones de circuito por omisión, debe ir al indicador de mandatos `BRS [i x][circuit defaults]Config>`.

Sintaxis:

deassign [*clase-prot* o *clase-filtro*]

Deassign-circuit

Nota: Sólo se utiliza en la configuración de Frame Relay.

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

Sintaxis:

deassign-c *número-circuito*

Default-circuit-class

Nota: Sólo se utiliza en la configuración de Frame Relay.

Utilice el mandato **default-circuit-class** en el nivel de interfaz para establecer 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 esta clase de circuitos, incluidos los huérfanos, que no están asignados a una clase-c de ancho de banda.

Sintaxis:

default-ci**rcuit-class**
nombre-clase %

Del-circuit-class

Nota: Sólo se utiliza en la configuración de Frame Relay.

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

Sintaxis:

del-ci**rcuit-class** *nombre-clase*

Default-class

Utilice el mandato **default-class** para establecer la clase-t y la prioridad por omisión en el valor que se quiera. Si no se había asignado ningún valor anteriormente, se utilizarán los valores por omisión del sistema. En caso contrario, se utilizará el último valor previamente asignado.

Nota: Si el mandato se ejecuta para un circuito Frame Relay que está utilizando actualmente definiciones de circuito por omisión para manejar clases de tráfico, se le preguntará si quiere alterar temporalmente las definiciones de circuito por omisión. Si la respuesta es afirmativa, el circuito se cambiará para que utilice las definiciones de circuito propias para manejar clases de tráfico, y se aceptará el mandato. Si la respuesta es "No", el mandato se cancelará anormalmente y el circuito seguirá utilizando las definiciones de circuito por omisión. Si quiere cambiar las definiciones de circuito por omisión, debe ir al indicador de mandatos `BRS [i x][circuit defaults]Config>`.

Sintaxis:

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

Del-class

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

Nota: Si el mandato se ejecuta para un circuito Frame Relay que está utilizando actualmente definiciones de circuito por omisión para manejar clases de tráfico, se le preguntará si quiere alterar temporalmente las definiciones de circuito por omisión. Si la respuesta es afirmativa, el circuito se cambiará para que utilice las definiciones de circuito propias para manejar clases de tráfico, y se aceptará el mandato. Si la respuesta es "No", el mandato se cancelará anormalmente y el circuito seguirá utilizando las definiciones de circuito por omisión. Si quiere cambiar las definiciones de circuito por omisión, debe ir al indicador de mandatos `BRS [i x][circuit defaults]Config>`.

Sintaxis:

del-**class** [*nombre-clase* o *número-clase*]

Disable

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

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

Sintaxis:

disable

Disable-hpr-over-ip-port-numbers

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

Sintaxis:

disable-h**pr-over-ip-port-numbers**

Para verificar que el filtrado de BRS del tráfico HPR sobre IP está inhabilitado, escriba el mandato **list**.

Nota: Si APPN está incluido en la imagen de carga, configure en el indicador de mandatos `APPN Config>` si se utilizará o no el tráfico HPR sobre IP.

Enable

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

Sintaxis:

enable

Nota:

- Si se configura BRS para una interfaz PPP, ejecute el mandato **enable** desde el indicador de interfaz y, a continuación, reinicie o vuelva a cargar el direccionador antes de configurar las clases de tráfico y asignarles protocolos y filtros.
- Si inicialmente se habilita BRS para un circuito Frame Relay, éste se inicializará con las definiciones de circuito por omisión para manejar clases de tráfico. Ejecute el mandato **enable** en el indicador de interfaz y en el indicador de circuito de todos los circuitos para los que quiera definir clases de tráfico. A continuación, reinicie o vuelva a cargar el direccionador, antes de configurar las clases de circuitos de la interfaz y las clases de tráfico de 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] [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>ex
Please reload  router for this command to take effect.
BRS [i 1] [dlci 16] Config>
```

Enable-hpr-over-ip-port-numbers

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

Nota: Si APPN está incluido en la imagen de carga, habilite HPR sobre IP y especifique los números de puerto UDP utilizados por el tráfico HPR sobre IP en el indicador de mandatos `APPN Config>`.

Sintaxis:

enable-h**pr-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

Este parámetro especifica el número de puerto UDP que utilizará el intercambio XID. Este número de puerto debe ser el mismo que el definido en otros dispositivos de la red.

Valores válidos: de 1024 a 65535

Valor por omisión: 12000

Network priority port number

Este parámetro especifica el número de puerto UDP que utilizará el tráfico con prioridad de red. Este número de puerto debe ser el mismo que el definido en otros dispositivos de la red.

Valores válidos: de 1024 a 65535

Valor por omisión: 12001

High exchange port number
Este parámetro especifica el número de puerto UDP que utilizará el tráfico con prioridad alta. Este número de puerto debe ser el mismo que el definido en otros dispositivos de la red.

Valores válidos: de 1024 a 65535

Valor por omisión: 12002

Medium exchange port number
Este parámetro especifica el número de puerto UDP que utilizará el tráfico con prioridad media. Este número de puerto debe ser el mismo que el definido en otros dispositivos de la red.

Valores válidos: de 1024 a 65535

Valor por omisión: 12003

Low exchange port number
Este parámetro especifica el número de puerto UDP que utilizará el tráfico con prioridad baja. Este número de puerto debe ser el mismo que el definido en otros dispositivos de la red.

Valores válidos: de 1024 a 65535

Valor por omisión: 12004

Interface

Utilice el mandato **interface** para elegir la interfaz serie a la que se referirán los mandatos de configuración de la reserva de ancho de banda. *Los direccionadores que ejecutan las interfaces PPP (protocolo punto a punto) y Frame Relay dan soporte a la reserva de ancho de banda.*

Sintaxis:

interface *número-interfaz*

Notas:

1. Si se quieren ejecutar mandatos de reserva de ancho de banda para otra interfaz, este mandato debe ejecutarse ***antes*** de utilizar ningún otro mandato de configuración de la reserva de ancho de banda. Si sale del indicador de la reserva de ancho de banda y quiere volver para hacer cambios en la reserva de ancho de banda de una interfaz previamente configurada, primero deberá volver a ejecutar este mandato.
2. Si se utiliza la función de restauración de WAN y el sistema BRS está configurado para una interfaz principal, BRS también deberá configurarse para la interfaz secundaria. Lo normal, cuando se utiliza la función de restauración de WAN, es que la interfaz secundaria adopte la identidad de la interfaz principal. Esto no es cierto para BRS; por lo tanto, BRS debe ser configurado tanto para la interfaz principal como para la secundaria.

Para habilitar la reserva de ancho de banda para una interfaz determinada, escriba en el indicador `BRS Config>` el número de la interfaz que da soporte al protocolo o función en particular. A continuación podrá utilizar el mandato de configuración de BRS **enable**, tal y como se describe en este capítulo. Para que el mandato entre en vigor, después de habilitar el número de interfaz deberá reiniciar o volver a

cargar el 2212 antes de poder hacer ningún otro cambio de configuración en la interfaz.

Notas:

1. Si está configurando BRS para una interfaz Frame Relay, se puede utilizar el mandato **circuit** para seleccionar circuitos y habilitar la reserva de ancho de banda para dichos circuitos antes de reiniciar o volver a cargar el direccionador.

List

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

Los mandatos **list** y **show** son parecidos. El mandato **list** muestra las definiciones almacenadas actualmente en la memoria SRAM y el mandato **show** muestra las definiciones almacenadas actualmente en la memoria RAM.

Sintaxis:

list *número-interfaz*

Dependiendo del indicador desde el que se ejecute el mandato **list**, la salida será diferente. Puede ejecutar 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: Si este mandato se ejecuta desde un indicador de circuito Frame Relay (`BRS [i x] [dlci y] Config>`), señalará si el circuito está utilizando las definiciones de circuito por omisión o las definiciones de circuito propias para manejar clases de tráfico. Si el circuito está utilizando las definiciones de circuito por omisión, se visualizarán las clases de tráfico y las asignaciones de protocolos, filtros e identificadores definidas actualmente para las definiciones de circuito por omisión. Sin embargo, para modificar las definiciones de circuito por omisión, deberá ir al indicador `BRS [i x] [circuit defaults] Config>`.

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

En el indicador de nivel de interfaz de BRS para Frame Relay, el mandato **list** muestra las clases de circuitos, sus porcentajes de ancho de banda configurados y los circuitos que tienen 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>
```

Ejemplo 2

```
 BRS [i 1] [dlci 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 CLASE1 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 de BRS. Cada clase de BRS tiene una prioridad asignada a sus protocolos, filtros e identificadores y cada cola de prioridad puede almacenar el número de paquetes especificado en este mandato.

Sintaxis:

q**ueue-length** *longitud-máxima longitud-mínima*

Este mandato establece el número máximo de almacenamientos intermedios que pueden ponerse en cada cola de prioridad de BRS, así como el número máximo que puede ponerse en cada cola de prioridad de BRS cuando el número de almacenamientos intermedios de entrada del direccionador es reducido.

Si ejecuta el mandato **queue-length** para una interfaz PPP los valores de longitud de cola se establecerán para todas las colas de prioridad de cada clase-t de BRS definida para la interfaz.

Si ejecuta el mandato **queue-length** para una interfaz Frame Relay (desde el indicador: `BRS [i 0] Config>`), los valores de longitud de cola por omisión se establecerán para todas las colas de prioridad de cada clase-t de BRS definida para los circuitos virtuales permanentes de la interfaz.

Si ejecuta el mandato **queue-length** para un PVC de Frame-Relay (desde un indicador parecido a este: `BRS [i 0] [dlci 16] Config>`), los valores de longitud de cola se establecerán para todas las colas de prioridad de cada clase-t de BRS definida para el PVC. Estos valores alteran temporalmente los valores de longitud de cola por omisión establecidos para la interfaz Frame Relay.

Attention: No ejecute este mandato, excepto que sea imprescindible. Los valores de longitud de cola por omisión son adecuados para la mayoría de usuarios. Si se establece una longitud de cola demasiado grande, es posible que el rendimiento del direccionador se degrade mucho.

Set-circuit-defaults

Utilice el mandato **set-circuit-defaults** para acceder a los mandatos que se utilizan para definir las definiciones de circuito por omisión para manejar clases de tráfico. Cualquier circuito Frame Relay de la interfaz que pueda utilizar las mismas clases de tráfico y asignaciones de protocolos, filtros e identificadores, puede utilizar dichas definiciones de circuito por omisión.

Sintaxis:

se**t-circuit-defaults**

Show

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

Sintaxis:

sh**ow** *número-interfaz*

Dependiendo del indicador en el que se ejecute el mandato **show**, la salida será diferente. Los indicadores desde los que se puede ejecutar el mandato **show** son los 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* del 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                   CLASE1              NORMAL            NO
ARP                  CLASE1              NORMAL            NO
DNA                  CLASE1              NORMAL            NO
VINES                CLASE1              NORMAL            NO
IPX                  CLASE1              NORMAL            YES
OSI                  CLASE1              NORMAL            NO
VOFR                 CLASE1              NORMAL            NO
AP2                  CLASE1              NORMAL            NO
ASRT                 DEFAULT             NORMAL            NO
NETBIOS              DEFAULT             NORMAL            NO
```

En el indicador de interfaz para PPP y en el indicador de circuito para Frame Relay, se muestra información sobre la clase de tráfico. En el indicador de interfaz para Frame Relay, se muestra información sobre la clase de circuito.

Notas:

1. Si este mandato se ejecuta desde un indicador de circuito Frame Relay (`BRS [i x] [dlci y] Config>`), indicará si el circuito está utilizando las definiciones de circuito por omisión o las definiciones de circuito propias para manejar clases de tráfico. Si el circuito está utilizando las definiciones de circuito por omisión, se visualizará la clase de tráfico y las asignaciones de protocolos, filtros e identificadores definidas actualmente para las definiciones de circuito por omisión. Sin embargo, para modificar las definiciones de circuito por omisión, deberá ir al indicador `BRS [i x] [circuit defaults] Config>`.
2. Este mandato no puede utilizarse desde el indicador `BRS [i x] [circuit defaults] Config>`.

Tag

Utilice el mandato **tag** para asignar un elemento filtro MAC al que se ha asignado un identificador durante la configuración de la función de filtrado MAC al primer nombre de identificador de BRS disponible. Los nombres de los identificadores de BRS son TAG1, TAG2, TAG3, TAG4 y TAG5. Utilice el nombre de identificador de

BRS en el mandato assign para asignar el identificador a una clase de tráfico de BRS.

Sintaxis:

t**ag** *número-ident_filtro_mac*

Utilice el mandato **list** para mostrar los identificadores de filtros MAC asignados a un nombre de identificador BRS y los nombres de identificadores BRS asignados a una clase de tráfico de ancho de banda.

Nota: Si el mandato se ejecuta para un circuito Frame Relay que está utilizando actualmente definiciones de circuito por omisión para manejar clases de tráfico, se le preguntará si quiere alterar temporalmente las definiciones de circuito por omisión. Si la respuesta es afirmativa, el circuito se cambiará para que utilice las definiciones de circuito propias para manejar clases de tráfico, y se aceptará el mandato. Si la respuesta es "No", el mandato se cancelará anormalmente y el circuito seguirá utilizando las definiciones de circuito por omisión. Si quiere cambiar las definiciones de circuito por omisión, debe ir al indicador de mandatos `BRS [i x][circuit defaults]Config>`.

Untag

Utilice el mandato **untag** para eliminar el número de identificador del filtro MAC y el nombre de identificador BRS asociado. Un identificador se puede eliminar solamente si el nombre de identificador BRS asociado no está asignado a una clase de tráfico de ancho de banda.

Sintaxis:

u**ntag** *ident_filtro_mac#*

Utilice el mandato **list** para mostrar los identificadores de filtros MAC asignados a un nombre de identificador BRS y los nombres de identificadores BRS asignados a una clase de tráfico de ancho de banda.

Nota: Si el mandato se ejecuta para un circuito Frame Relay que está utilizando actualmente definiciones de circuito por omisión para manejar clases de tráfico, se le preguntará si quiere alterar temporalmente las definiciones de circuito por omisión. Si la respuesta es afirmativa, el circuito se cambiará para que utilice las definiciones de circuito propias para manejar clases de tráfico, y se aceptará el mandato. Si la respuesta es "No", el mandato se cancelará anormalmente y el circuito seguirá utilizando las definiciones de circuito por omisión. Si quiere cambiar las definiciones de circuito por omisión, debe ir 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 de circuito propias y utilizar las definiciones de circuito por omisión para manejar clases de tráfico. Se le pedirá que confirme si quiere utilizar las definiciones de circuito por omisión.

Sintaxis:

us**e-circuit-defaults**

Notas:

1. Este mandato se utiliza solamente en la configuración de Frame Relay
2. Para que los valores por omisión sean operativos, deberá reiniciar o volver a cargar el direccionador.

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 para supervisar la reserva de ancho de banda del direccionador, siga estos pasos:

1. En el indicador OPCON prompt (*), escriba **talk 5**.
2. En el indicador GWCON prompt (+), escriba **feature brs.**
3. En el indicador BRS>, escriba **interface #**, donde # es el número de interfaz que quiere supervisar. Esto le llevará al indicador de nivel de interfaz de BRS, BRS [i x]>, donde x es el número de interfaz.
4. Sólo para Frame Relay, escriba **circuit #** en el indicador de interfaz para especificar el circuito de esta interfaz que se quiere supervisar.

   Esto le llevará 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 apropiado (consulte el apartado “Mandatos de supervisión de la reserva de ancho de banda”).

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

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

   El mandato **interface #** selecciona la interfaz concreta que se quiere supervisar para la reserva de ancho de banda.

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

   Siempre puede volver al indicador GWCON escribiendo el mandato **exit** en el indicador BRS>.

   Una vez en el indicador de supervisión de la reserva de ancho de banda (BRS>), puede entrar cualquiera de los mandatos de supervisión que se describen en la Tabla 4 en la página 51.

Mandatos de supervisión de la reserva de ancho de banda

En este apartado se resumen los mandatos de supervisión de la reserva de ancho de banda y, a continuación, se explican con más detalle. La 4 muestra los mandatos de supervisión de la reserva de ancho de banda. Los mandatos que

pueden utilizarse varían dependiendo del indicador de supervisión de BRS (BRS>, BRS [i x]> o BRS [i x] [dlci y]>) desde el que se ejecuten.

Tabla 4. Resumen de mandatos de supervisión de la reserva de ancho de banda

Mandato	Utilizado sólo con FR	Función
? (Ayuda)		Visualiza todos los mandatos disponibles en este nivel de mandato o lista las opciones de un mandato concreto (si está disponible). Consulte el apartado "Obtención de ayuda" en la página xxv
Circuit	sí	Selecciona el DLCI de un circuito virtual permanente (PVC) de Frame Relay. Para supervisar la reserva de ancho de banda del tráfico de Frame Relay, debe estar en el nivel de indicador de circuito.
Clear		Borra los contadores actuales de las clases-t y los almacena como contadores **last** de las clases-t. Los contadores se listan por clase.
Clear-circuit-class	sí	Borra los contadores actuales de las clases-c y los almacena como contadores **last** de las clases-c. Los contadores se listan por clase.
Counters		Visualiza los contadores actuales de las clases-t.
Counters-circuit-class	sí	Visualiza los contadores actuales de las clases-c.
Interface		Selecciona la interfaz a supervisar. **Nota:** Este mandato debe ejecutarse antes de utilizar cualquier mandato de supervisión de reserva de ancho de banda.
Last		Visualiza los últimos contadores que se guardaron de las clases-t.
Last-circuit-class	sí	Visualiza los últimos contadores que se guardaron de las clases-c.
Exit		Vuelve al nivel de mandatos anterior. Consulte el apartado "Salida de un entorno de nivel inferior" en la página xxv

Circuit

Nota: Sólo se utiliza en la supervisión de Frame Relay.

Utilice el mandato **circuit** para seleccionar el DLCI de un PVC de Frame Relay que se quiere supervisar. Este mandato sólo puede ejecutarse desde el indicador de supervisión de interfaz de BRS (BRS [i #]>).

Sintaxis:

circuit *circuito-virtual-permanente-#*

de seleccionar el circuito Frame Relay, se podrán utilizar los mandatos siguientes desde el indicador de circuito:

```
CLEAR
COUNTERS
LAST
EXIT
```

Clear

Utilice el mandato **clear** para guardar los contadores actuales de las clases-t de la reserva de ancho de banda (de manera que puedan recuperarse con el mandato **last**) y borrar los valores. Los contadores se guardan por clase de tráfico de ancho de banda.

Sintaxis:

clear

Clear-Circuit-Class

Nota: Sólo se utiliza en la supervisión de Frame Relay.

Utilice el mandato **clear-circuit-class** para guardar los contadores actuales de las clases-c de la reserva de ancho de banda (de manera que puedan recuperarse con el mandato **last-circuit-class**) y borrar los valores. Los contadores se guardan por clase de circuito.

Sintaxis:

clear-c**ircuit-class**

Counters

Utilice el mandato **counters** para mostrar las estadísticas que describen el tráfico de la reserva de ancho de banda de 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
   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
   LOW               0              0             0            0        0
   NORMAL           20           5020             0            0        0
   HIGH              0              0             0            0        0
   URGENT           35            535             0            0        0
CLASE_1              5            910             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
CLASE_2             70           4123             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 por paquete que no han podido transmitirse porque se ha alcanzado la longitud máxima de una cola de prioridad o porque el paquete no ha podido ponerse en

cola, ya que la cola de prioridad estaba en el umbral mínimo de longitud de cola y el paquete provenía de una interfaz que estaba quedándose sin almacenamientos intermedios de recepción.

Pkt Ovfl
Lista el número de paquetes que no han podido transmitirse porque se ha alcanzado la longitud máxima de una cola de prioridad o porque el paquete no ha podido ponerse en cola, ya que la cola de prioridad estaba en el umbral mínimo de longitud de cola y el paquete provenía de una interfaz que estaba quedándose sin almacenamientos intermedios de recepción.

Q_len El número actual de paquetes que esperan ser transmitidos en cada cola de prioridad para cada clase de tráfico.

Counters-circuit-class

Nota: Sólo se utiliza en la supervisión de Frame Relay.

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

Sintaxis:

counters-c**ircuit-class**

Ejemplo:

```
counters-circuit-class

Bandwidth Reservation Circuit Class Counters
Interface 1


Class         Pkt Xmit     Bytes Xmit     Bytes Ovfl
DEFAULT             25           3402             26
CIRCLASE1            1             56              0
CIRCLASE2            0              0              0

TOTAL               26           3458             26
```

Interface

Utilice el mandato **interface** para seleccionar la interfaz serie a la que se referirán los mandatos de supervisión de la reserva de ancho de banda. *Los direccionadores que ejecutan las interfaces PPP (protocolo punto a punto) y Frame Relay dan soporte la reserva de ancho de banda.*

Sintaxis:

i**nterface** *número-interfaz*

Nota: Si se quieren entrar mandatos de reserva de ancho de banda para una interfaz nueva, este mandato debe ejecutarse antes de utilizar cualquier mandato de supervisión de la reserva de ancho de banda. Si sale del indicador de supervisión de la reserva de ancho de banda (BRS>) y quiere volver a supervisar la reserva de ancho de banda, primero deberá volver a entrar este mandato.

Para supervisar la reserva de ancho de banda para una interfaz en particular, escriba el número de la interfaz en el indicador de supervisión BRS>. A continuación podrá utilizar los mandatos de supervisión de reserva de ancho de banda que se describen en este capítulo.

Last

Utilice el mandato **last** para visualizar las últimas estadísticas que se guardaron de las clases-t. Las estadísticas de las clases-t se muestran en el mismo formato que las del mandato **counters**.

Sintaxis:

last

Last-circuit-class

Nota: Sólo se utiliza en la supervisión de Frame Relay.

Utilice el mandato **last-circuit-class** para visualizar las últimas estadísticas que se guardaron de las clases de circuitos. Las estadísticas de las clases-c se muestran en el mismo formato que las del mandato **counters-circuit-class**.

Sintaxis:

last-c**ircuit-class**

Capítulo 3. Utilización del filtrado MAC

En este capítulo se describe cómo utilizar el control de acceso al medio (MAC) para especificar filtros de paquetes que se aplicarán a los paquetes durante el proceso. Consta de los apartados siguientes:

- "Filtros MAC y tráfico DLSw"
- "Parámetros del filtrado MAC" en la página 56

Un filtro es un conjunto de reglas que se aplican a un paquete para determinar cómo manejarlo durante la transmisión por un puente. Los filtros MAC afectan únicamente al tráfico que se transmite por puentes.

Nota: Se permite el filtrado MAC del tráfico transmitido por túneles.

Durante el proceso de filtrado, los paquetes se procesan, se filtran o se identifican durante la transmisión por el puente. Las acciones son:

- **Procesado** – Se permite que los paquetes atraviesen el puente sin ser afectados.
- **Filtrado** – No se permite que los paquetes atraviesen el puente.
- **Identificado** – Se permite que los paquetes atraviesen el puente, pero se identifican con un número comprendido entre 1 y 64, que depende de un parámetro configurable.

Un filtro MAC consta de los tres objetos siguientes:

1. Elemento filtro – regla única que se aplica al campo dirección o a una ventana arbitraria de datos de un paquete. El resultado de aplicar la regla es una condición verdadera (la comparación es satisfactoria) o falsa (no coincide).
2. Lista de filtros – lista de una o más elementos filtro.
3. Filtro – conjunto de listas de filtros.

Filtros MAC y tráfico DLSw

Se puede filtrar el tráfico LLC entrante para la red DLSw implementando filtros MAC.

Para configurar un filtro para LLC, utilice el número de *red de puente* como número de interfaz del filtro. El número de red de puente se calcula sumando dos al número de interfaces configuradas por el direccionador. Para ver una lista de las interfaces, escriba el mandato **list devices** en el indicador `Config>`, o escriba **configuration** en el indicador +.

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
```

Cuando se configura un filtro para la red de puente, por ejemplo, el direccionador no descartará las tramas que coincidan con filtros de exclusión. Al contrario, reenviará las tramas al puente.

Parámetros del filtrado MAC

Para crear un filtro, se pueden especificar algunos o todos los parámetros siguientes:

- Dirección MAC origen o destino
- Datos que se compararán en el paquete
- Máscara que se aplicará a los campos del paquete que se van a filtrar
- Número de interfaz
- Clase Input u Output
- Clase Include, Exclude o Tag
- Valor de identificador (si se da la clase Identificar)

Parámetros de los elementos filtro

Los parámetros siguientes se utilizan para crear un elemento filtro de dirección:

- Tipo de dirección: SOURCE o DESTINATION
- Identificador: un *valor de identificador*
- Máscara de dirección: una *máscara hexadecimal*

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

La máscara de dirección es una serie de números hexadecimales, que sirve para comparar las direcciones del paquete. La máscara se aplica a la dirección MAC (SOURCE o DESTINATION) del paquete antes de compararla con la dirección MAC especificada.

La longitud de la máscara de dirección debe ser igual a la de la dirección MAC. Se realizará una operación AND lógica entre los bytes especificados por la máscara de dirección y los bytes de la dirección MAC, antes de comparar si es igual a la dirección MAC especificada. Si no se especifica ninguna máscara, se supondrá que todos son 1.

Parámetros de las listas de filtros

Los parámetros siguientes se utilizan para crear una lista de filtros:

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

A partir de uno o más elementos filtro se crea una lista de filtros. A cada lista de filtros se le asigna un nombre único.

Aplicar una lista de filtros a un paquete consiste en comparar cada elemento filtro en el orden en que se añadieron a la lista. Si un elemento filtro de la lista devuelve una condición TRUE (verdadera), la lista de filtros devolverá la acción que se le ha asignado.

Parámetros de los filtros

Los parámetros siguientes se utilizan para crear un filtro:

- Nombres de listas de filtros: *serie de caracteres ASCII 1. . . serie de caracteres ASCII n*
- Número de interfaz: un *número de IFC*
- Sentido del puerto: INPUT u OUTPUT

- Acción por omisión: INCLUDE, EXCLUDE o TAG
- Identificador por omisión: un *valor de identificador*

Un filtro se crea asociando un grupo de nombres de listas de filtros con un número de interfaz y asignando una clase INPUT u OUTPUT. Aplicar un filtro a un paquete significa que debe aplicarse cada una de las listas de filtros asociadas a los paquetes que se reciben (INPUT) o que se envían (OUTPUT) para el número de interfaz especificada.

Si al evaluar un paquete, un filtro obtiene una condición INCLUDE, el paquete se reenvía. Si al evaluar un paquete, un filtro obtiene una condición EXCLUDE, el paquete se descartará. Si al evaluar un paquete, un filtro obtiene una condición TAG, el paquete se reenviará con un identificador.

Un parámetro adicional para cada filtro es la acción por omisión, que se ejecutará en caso de que ninguna de las comparaciones realizadas con sus listas de filtros haya sido satisfactoria. La acción por omisión es INCLUDE. Puede establecerse como INCLUDE, EXCLUDE o TAG. Si la acción por omisión es TAG, además tendrá que establecerse un valor de identificador.

Utilización de identificadores del filtrado MAC

En la lista siguiente se describen algunos usos de los identificadores del filtrado MAC:

- La reserva de ancho de banda y la función filtrado MAC (MCF) manejan conjuntamente el filtrado de direcciones MAC utilizando identificadores. Por ejemplo, un usuario con reserva de ancho de banda puede categorizar el tráfico que pasa por un puente asignándole un identificador.
- El proceso de identificación consiste en crear un elemento filtro en la consola de configuración del filtrado MAC y asignarle un identificador. A continuación, el identificador se utiliza para configurar una clase de ancho de banda para todos los paquetes asociados con este identificador. El valor de los identificadores debe estar comprendido entre 1 y 64.
- Una vez creado un filtro con identificador en el proceso de configuración de filtros MAC, se utiliza el mandato **tag** de la reserva de ancho de banda (BRS) para asignar un nombre de identificador de BRS (TAG1, TAG2, TAG3, TAG4 o TAG5) al número de identificador del filtro MAC. A partir de ahora, el nombre de identificador de BRS se utilizará en el mandato de configuración **assign** de BRS para asignar el filtro MAC correspondiente a una clase de tráfico y prioridad de ancho de banda.
- Se pueden establecer hasta 5 direcciones MAC con identificador, con valores de 1 a 5. En primer lugar se buscará TAG1, después TAG2, y así sucesivamente hasta TAG5.

Los identificadores también pueden hacer referencia a “grupos” de un Túnel IP. Los extremos de un Túnel IP pueden pertenecer a un número indeterminado de grupos, y recibir paquetes asignados a un grupo concreto mediante la función de identificación de filtros de direcciones MAC.

Utilización del filtrado MAC

Capítulo 4. Configuración y supervisión del filtrado MAC

En este capítulo se describe cómo acceder a los indicadores de configuración y supervisión del filtrado MAC y cómo utilizar los mandatos disponibles. Consta de los apartados siguientes:

- "Acceso al indicador de supervisión del filtrado MAC" en la página 67
- "Mandatos de supervisión del filtrado MAC" en la página 67

Acceso al indicador de configuración del filtrado MAC

Utilice el mandato **feature** desde el proceso CONFIG para acceder a los mandatos de configuración del filtrado MAC. El mandato **feature** le permite acceder a los mandatos de configuración de determinadas funciones externas al protocolo y a los procesos de configuración de la interfaz de red.

Para obtener una lista de las funciones disponibles en este release del software, escriba un interrogante después del mandato **feature**. 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 función* (3) o del *nombre corto* (MCF). Por ejemplo:

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

Una vez se accede al indicador de configuración del filtrado MAC, pueden empezarse a entrar mandatos específicos de configuración. Siempre puede volver al indicador CONFIG escribiendo el mandato **exit** en el indicador de configuración del filtrado MAC.

Mandatos de configuración del filtrado MAC

En este apartado se resumen los mandatos de configuración del filtrado MAC. Escriba los mandatos en el indicador `Filter config>`.

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

Tabla 5 (Página 1 de 2). Resumen de mandatos de configuración del filtrado MAC

Mandato	Función
? (Ayuda)	Visualiza todos los mandatos disponibles para este nivel de mandato, o lista las opciones de mandatos específicos (si es que están disponibles). Consulte "Obtención de ayuda" en la página xxv.
Attach	Añade una lista de filtros a un filtro.
Create	Crea una lista de filtros o un filtro INPUT u OUTPUT.
Default	Establece para el filtro especificado la acción por omisión: EXCLUDE, INCLUDE o TAG.
Delete	Elimina toda la información asociada con una lista de filtros. También suprime un filtro creado con el mandato create.
Detach	Elimina una lista de filtros de un filtro.

Tabla 5 (Página 2 de 2). Resumen de mandatos de configuración del filtrado MAC

Mandato	Función
Disable	Inhabilita totalmente el filtrado MAC, o inhabilita un filtro determinado.
Enable	Habilita totalmente el filtrado MAC, o habilita un filtro determinado.
List	Muestra un resumen de todas las listas de filtros y filtros configuradas por el usuario. También genera una lista de las listas de filtros conectadas con este filtro y toda la información correspondiente al filtro.
Move	Reordena las listas de filtros conectadas con un filtro determinado.
Reinit	Reinicializa todo el sistema de filtrado MAC después de haber actualizado la configuración, sin afectar al resto del direccionador.
Set-Cache	Cambia el tamaño de la antememoria de un filtro.
Update	Añade o suprime información de una lista de filtros determinada. Le lleva al menú de submandatos apropiado.
Exit	Hace volver al nivel de mandato anterior. Consulte “Salida de un entorno de nivel inferior” en la página xxv.

Attach

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

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

Sintaxis:

att**ach** *nombre-lista-filtros número-filtro*

Create

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

Sintaxis:

c**reate** list *nombre-lista-filtros*

filter [input u output] *número-interfaz*

list *nombre-lista-filtros*

Crea una lista de filtros. El usuario debe dar nombre a la lista, que consiste en una serie de caracteres (nombre-lista-filtros) exclusiva de hasta 16 caracteres de longitud. Este nombre sirve para identificar la lista de filtros que se va a crear. Además, lo utilizan otros mandatos asociados con la lista de filtros.

filter [input u output] *número-interfaz*

Crea un filtro y lo pone en la red asociada con el sentido de entrada (INPUT) o salida (OUTPUT) de la interfaz indicada por el número de interfaz. Por omisión, este filtro se crea sin listas de filtros conectadas, su acción por omisión es INCLUDE y está habilitado (ENABLED).

Default

Utilice el mandato **default** para establecer la acción por omisión del filtro (exclude, include o tag) especificado por un número de filtro.

Sintaxis:

def**ault** exclude *número-filtro*
include *número-filtro*
tag *número-ident número-filtro*

exclude *número-filtro*
Establece la acción por omisión del filtro (especificado por un número de filtro) como exclude.

include *número-filtro*
Establece la acción por omisión del filtro (especificado por un número de filtro) como include.

tag *número-ident número-filtro*
Establece la acción por omisión del filtro (especificado por un número de filtro) como TAG, y establece como número de identificador el valor de identificador asociado.

Delete

Utilice el mandato **delete** para eliminar toda la información asociada con una lista de filtros y para liberar la serie de caracteres asignada a la lista, de forma que pueda volver a utilizarse para nombrar una lista de filtros nueva. Si la lista de filtros está conectada a un filtro ya existente creado por el usuario, este mandato mostrará un mensaje de error en la consola y no eliminará nada. También se eliminarán todos los elementos filtro que pertenezcan a la lista.

Además, este mandato también elimina los filtros creados con el mandato **create filter**.

Sintaxis:

del**ete** list *lista-filtros*
filter *número-filtro*

list *lista-filtros*
Elimina toda la información asociada con una lista de filtros y libera la serie de caracteres asignada a la lista, de forma que pueda volver a utilizarse para nombrar una lista de filtros nueva. La lista de filtros debe ser una serie de caracteres entrada anteriormente en un mandato **create list**.

Si la lista de filtros está conectada a un filtro ya existente creado por el usuario, el mandato mostrará un mensaje de error en la consola y no eliminará nada. Además, cuando se ejecute el mandato, también se eliminarán todos los elementos filtro que pertenezcan a la lista.

filter *número-filtro*
Suprime un filtro creado con el mandato **create filter**.

Detach

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

Sintaxis:

det**ach** *nombre-lista-filtros número-filtro*

Disable

Utilice el mandato **disable** para inhabilitar totalmente el filtrado MAC, o para inhabilitar un filtro determinado.

Sintaxis:

disable all

filter *número-filtro*

all Inhabilita totalmente el filtrado MAC. Sin embargo, si los filtros se habilitaron previamente, seguirán estando habilitados (ENABLED).

filter *número-filtro*
Inhabilita un filtro determinado. El parámetro número-filtro se corresponde con los números mostrados al ejecutar el mandato **list filters**.

Enable

Utilice el mandato **enable** para habilitar totalmente el filtrado MAC, o para habilitar un filtro determinado.

Sintaxis:

enable all

filter *número-filtro*

all Habilita totalmente el filtrado MAC, aunque es posible que los propios filtros estén inhabilitados (DISABLED).

filter *número-filtro*
Habilita un filtro determinado. El parámetro número-filtro se corresponde con los números mostrados al ejecutar el mandato **list filters**.

List

Utilice el mandato **list** para mostrar un resumen de todos los filtros y listas de filtros configurados por el usuario. No se muestra la lista de todas las listas de filtros conectadas a un filtro. También se muestra la información siguiente:

- Una lista que contiene el estado del sistema de filtrado (ENABLE, DISABLE)
- El conjunto de registros de las listas de filtros configuradas
- Todos los registros de los filtros configurados.

Además, se muestra la información siguiente para cada filtro:

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

Por último, también genera una lista de las listas de filtros conectadas con este filtro y toda la información correspondiente al filtro.

Sintaxis:

list all

filter *número-filtro*

all Muestra un resumen de todas las listas de filtros y filtros configuradas.

filter *número-filtro*

Genera una lista de listas de filtros conectadas con el filtro especificado y toda la información correspondiente al filtro.

Move

Utilice el mandato **move** para reordenar las listas de filtros conectadas al filtro especificado (por un parámetro número-filtro). La lista especificada por el nombre-lista-filtros1 se coloca inmediatamente delante de la lista especificada por el nombre-lista-filtros2.

Sintaxis:

m**ove** *nombre-lista-filtros1 nombre-lista-filtros2 número-filtro*

Reinit

Utilice el mandato **reinit** para reinicializar todo el sistema de filtrado MAC después de haber actualizado la configuración, sin afectar al resto del direccionador.

Sintaxis:

r**einit**

Set-Cache

Utilice el mandato **set-cache** para cambiar el tamaño por omisión de la antememoria (16) a un número comprendido entre 4 y 32768.

Sintaxis:

s**et-cache** *tamaño-antememoria número-filtro*

Update

Utilice el mandato **update** para añadir o eliminar información de una lista de filtros determinada. Si utiliza este mandato con el nombre-lista-filtros deseado, le llevará al indicador `Filter nombre-lista-filtros Config>` de la lista de filtros especificada. Desde este nuevo indicador se puede cambiar la información de la lista especificada.

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

Sintaxis:

u**pdate** *nombre-lista-filtros*

Submandatos de actualización

Es este apartado se resumen los submandatos de configuración del filtrado MAC. Estos submandatos se escriben en el indicador `Filter nombre-lista-filtros config>`.

Tabla 6. Resumen de submandatos de actualización

Submandato	Función
? (Ayuda)	Visualiza todos los mandatos disponibles para este nivel de mandato, o lista las opciones de mandatos específicos (si es que están disponibles). Consulte “Obtención de ayuda” en la página xxv.
Add	Añade filtros de direcciones MAC origen y destino o un filtro de ventana. Añade elementos filtro a una lista de filtros.
Delete	Elimina elementos filtro de una lista de filtros.
List	Muestra un resumen de todas las listas de filtros y filtros configuradas por el usuario. También genera una lista de las listas de filtros conectadas con este filtro y toda la información correspondiente al filtro.
Move	Reordena las listas de filtros conectadas al filtro especificado.
Set-Action	Configura un elemento filtro para que evalúe la condición INCLUDE, EXCLUDE o TAG (con una opción número identificador).
Exit	Hace volver al nivel de mandato anterior. Consulte “Salida de un entorno de nivel inferior” en la página xxv.

Utilice los submandatos siguientes para actualizar una lista de filtros.

Add

Utilice el submandato **add** para añadir elementos filtro a una lista de filtros. Este submandato le permite añadir un número hexadecimal que se comparará con la dirección MAC origen o destino, o una secuencia de datos de ventana con una máscara que se comparará con los datos de un paquete.

Es importante el orden en que se añadan los elementos filtro a una lista de filtros dada, ya que determina el orden en que se aplicarán a un paquete.

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

La primera coincidencia que se produzca interrumpirá la aplicación de los elementos filtro y la lista de filtros evaluará la condición INCLUDE, EXCLUDE o TAG, dependiendo de la acción asignada en la lista de filtros. Si ninguna de las comparaciones de los elementos filtro de la lista de filtros produce una coincidencia, se devolverá la acción por omisión (INCLUDE, EXCLUDE o TAG) del filtro.

Sintaxis: a**dd** source *dir-MAC-hex máscara-hex*
destination *dir-MAC-hex máscara-hex*
window MAC *valor-desplaz datos-hex máscara-hex*
window INFO *valor-desplaz datos-hex máscara-hex*

source *dir-MAC-hex máscara-hex*
Añade un número hexadecimal que se comparará con la dirección MAC. El valor ***dir-MAC-hex*** debe ser un número par de dígitos hexadecimales de, como máximo, 16 dígitos de longitud y debe escribirse sin el prefijo 0x.

El parámetro máscara-hex debe ser de la misma longitud que la dirección MAC hexadecimal, y se realiza una operación AND lógica entre éste y la

dirección MAC del paquete. El argumento máscara-hex por omisión es una serie de unos binarios.

El orden de bits del parámetro dir-MAC-hex puede especificarse en forma canónica o no canónica. El orden de bits canónico se especifica como un número hexadecimal (por ejemplo, 000003001234). También puede representarse como una serie de pares de dígitos hexadecimales separados por guiones (-) (por ejemplo, 00-00-03-00-12-34).

Un orden de bits no canónico se especifica como una serie de pares de dígitos hexadecimales separados por el signo de dos puntos (por ejemplo, 00:00:C9:09:66:49). Las direcciones MAC de los elementos filtro siempre se mostrarán con guiones (-) o el signo de dos puntos (:) para distinguir las representaciones canónica y no canónica.

destination *dir-MAC-hex máscara-hex*
Actúa de la misma forma que el submandato **add source** excepto que la comparación se hace con la dirección MAC destino del paquete, en lugar de hacerse con la dirección origen.

window MAC *valor-desplaz datos-hex máscara-hex*
Añade un elemento filtro de ventana corredera que utiliza el desplazamiento especificado (calculado a partir del inicio de la trama) que compara los datos hexadecimales de la máscara, con los datos del paquete.

window INFO *valor-desplaz datos-hex máscara-hex*
Similar al mandato **add window mac** excepto que el desplazamiento se calcula respecto al inicio del campo información.

Delete

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

Cuando se ejecuta el submandato **delete**, se cubre cualquier hueco creado en la secuencia de números. Por ejemplo, si existen los elementos filtro 1, 2, 3 y 4, y se elimina el elemento filtro 3, el elemento filtro número 4 se volverá a numerar como 3.

Sintaxis:

de**lete** *número-elemento-filtro*

List

Utilice el submandato **list** para imprimir una lista de todos los registros de elementos filtro. Se mostrará la información siguiente de cada elemento filtro de direcciones MAC:

- dirección MAC y máscara de dirección en forma canónica y no canónica.
- números de los elementos filtro
- tipo de dirección (origen o destino)
- acción de la lista de filtros

Sintaxis:

l**ist** canonical
noncanonical
mac-address canonical

mac-address noncanonical

window

canonical
Imprime una lista de todos los registros de los elementos filtro de una lista de filtros, en la que aparecen los números de elemento, el tipo de dirección (SRC, DST), la dirección MAC y la máscara de dirección en forma canónica. También aparece la acción de la lista de filtros.

mac-address canonical
Imprime una lista de todos los registros de los elementos filtro de una lista de filtros, en la que aparecen los números de elemento, el tipo de dirección (SRC, DST), la dirección MAC y la máscara de dirección en forma canónica. Además, aparece la acción de la lista de filtros.

noncanonical
Imprime una lista de todos los registros de los elementos filtro de una lista de filtros, en la que aparecen los números de elemento, el tipo de dirección (SRC, DST), y la dirección MAC y la dirección de máscara en forma no canónica. También aparece la acción de la lista de filtros.

mac-address noncanonical
Imprime una lista de todos los registros de los elementos filtro de una lista de filtros, en la que aparecen los números de elemento, el tipo de dirección (SRC, DST), y la dirección MAC y la dirección de máscara en forma no canónica. También aparece la acción de la lista de filtros.

window
Imprime una lista de todos los registros de los elementos filtro de la ventana corredera de la lista de filtros, en la que aparecen los números de elemento, la base, el desplazamiento, los datos y la máscara. También aparece la acción de la lista de filtros.

Move

El submandato **move** reordena los elementos filtro de la lista de filtros. El número del elemento filtro especificado por el *nombre-elemento-filtro1* se coloca junto antes que el *nombre-elemento-filtro2* y se vuelve a numerar.

Sintaxis:

m**ove** *nombre-elemento-filtro1 nombre-elemento-filtro2*

Set-Action

El submandato **set-action** le permite configurar un elemento filtro para que evalúe una de las condiciones INCLUDE, EXCLUDE o TAG (con una opción número identificador). Si la comparación entre uno de los elementos filtro de la lista de filtros y el contenido del paquete que se está considerando si filtrar o no, es satisfactoria, la lista de filtros evaluará la condición especificada. El valor por omisión es INCLUDE.

Sintaxis:

s**et-action** [INCLUDE o EXCLUDE o TAG] *número-identificador*

Acceso al indicador de supervisión del filtrado MAC

Utilice el mandato **feature** desde el proceso GWCON para acceder a los mandatos de supervisión del filtrado MAC. El mandato **feature** le permite acceder a los mandatos de supervisión de determinadas funciones del direccionador, externas al protocolo y a los procesos de supervisión de la interfaz de red.

Para obtener una lista de las funciones disponibles en este release del software, escriba un interrogante después del mandato **feature**. Por ejemplo:

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

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

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

Una vez se accede al indicador de supervisión del filtrado MAC, pueden empezarse a entrar mandatos específicos de supervisión. Siempre se puede volver al indicador GWCON escribiendo el mandato **exit** en el indicador de supervisión del filtrado MAC.

Mandatos de supervisión del filtrado MAC

En este apartado se resumen los mandatos de supervisión del filtrado MAC. Entre estos mandatos en el indicador `Filter>`.

Tabla 7. Resumen de mandatos de supervisión del filtrado MAC

Mandato	Función
? (Ayuda)	Visualiza todos los mandatos disponibles para este nivel de mandato, o lista las opciones de mandatos específicos (si es que están disponibles). Consulte “Obtención de ayuda” en la página xxv.
Clear	Borra las estadísticas de "un filtro" listadas en el mandato list filter.
Disable	Inhabilita globalmente el filtrado MAC o "un filtro".
Enable	Habilita globalmente el filtrado MAC o "un filtro".
List	Muestra un resumen de las estadísticas y valores de cada filtro que se está ejecutando actualmente en el direccionador.
Reinit	Reinicializa todo el sistema de filtrado MAC después de haber actualizado la configuración, sin afectar al resto del direccionador.
Exit	Hace volver al nivel de mandato anterior. Consulte “Salida de un entorno de nivel inferior” en la página xxv.

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

Clear

Utilice el mandato **clear** para borrar las estadísticas de filtros.

Sintaxis:

clear all
filter *número-filtro*

all Borra las estadísticas que se listan en el mandato **list all**.

filter *número-filtro*
Borra las estadísticas que se listan en el mandato **list filter**.

Disable

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

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

Sintaxis:

disable all

filter *número-filtro*

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

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 indica 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 individualmente cada filtro.

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

Sintaxis:

enable all

filter *número-filtro*

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

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 indica ningún número de filtro, el filtrado MAC se habilita globalmente.

List

Utilice el mandato **list** para mostrar un resumen de las estadísticas y valores de cada filtro que se está ejecutando actualmente en el direccionador. Cundo se ejecuta el mandato **list all**, se muestra la información siguiente de cada filtro:

- Acción por omisión
- Tamaño de la antememoria
- Identificador por omisión
- Estado (habilitado/inhabilitado)
- Número de paquetes filtrados como INCLUDE, EXCLUDE o TAG.

Además, si se ejecuta el mandato **list filter**, se muestra la información siguiente del filtro especificado:

- Toda la información que se muestra al ejecutar el mandato list all
- Todas las listas de filtros que se están ejecutando actualmente para este filtro:
  - Nombre de la lista
  - Acción de la lista
  - Identificador de la lista
  - Número de paquetes filtrados por cada lista de filtros.

Sintaxis:

list all

filter *número-filtro*

all Lista las estadísticas y valores de cada filtro que se está ejecutando actualmente en el direccionador.

filter *número-filtro*
Genera estadísticas y valores para cada filtro además de para todas las listas de filtros que se están ejecutando actualmente en el direccionador.

Reinit

Utilice el mandato **reinit** para reinicializar todo el sistema de filtrado MAC después de haber actualizado la configuración, sin afectar al resto del direccionador.

Sintaxis:

reinit

Configuración del filtrado MAC

Capítulo 5. Utilización de la restauración de WAN

Este capítulo consta de los apartados siguientes:

- "Visión general de las características restauración de WAN, redireccionamiento de WAN y marcación por desbordamiento"
- "Antes de empezar" en la página 73
- "Procedimiento de configuración de la restauración de WAN" en la página 74
- "Configuración del circuito de marcación secundario" en la página 74

Visión general de las características restauración de WAN, redireccionamiento de WAN y marcación por desbordamiento

Las características restauración de WAN, redireccionamiento de WAN y marcación por desbordamiento tienen funciones parecidas y pueden confundirse. La intención de este apartado es ayudarle a decidir cuál de estas características le será útil y a encontrar la información necesaria para configurarlas.

En el capítulo "Configuración de la restauración de WAN" encontrará los mandatos de configuración de las tres características. Para obtener información adicional sobre las características redireccionamiento de WAN y marcación por desbordamiento, consulte el Capítulo 7, "La característica de redireccionamiento de WAN" en la página 97.

restauración de WAN

La restauración de WAN es la función más básica. Al utilizar esta función, se configura un enlace principal y uno secundario. En el caso de que el enlace principal diera un error, se arrancaría el enlace secundario, que asumiría las características del principal. En el enlace secundario no se configura ninguna definición de protocolos, puesto que utiliza las del enlace principal.

Para la restauración de WAN:

- El enlace principal y el secundario están conectados.
- Sólo se puede configurar un enlace principal para que utilice un enlace secundario determinado.
- En el enlace secundario no se configura ninguna definición de protocolos (por ejemplo: direcciones de protocolos).
- El enlace principal puede ser una interfaz PPP serie o una interfaz PPP multienlace. No puede ser una interfaz PPP de circuito de marcación.
- El enlace secundario debe ser una interfaz PPP de circuito de marcación o multienlace.
- Se debe habilitar la característica WRS ejecutando el mandato **enable wrs**.
- Se debe habilitar la conexión entre los enlaces principal y secundario ejecutando el mandato **enable secondary-circuit**.

Nota: Si BRS está configurado para un enlace principal y éste es parte de una conexión entre el enlace principal y el secundario para la restauración de WAN, deberá configurar BRS para el enlace secundario. Lo normal, cuando se configura la característica de restauración de WAN, es que el enlace secundario adopte la identidad del enlace principal. Sin embargo, esto no es

cierto para BRS; por lo tanto, BRS debe configurarse tanto para el enlace principal, como para el enlace secundario.

redireccionamiento de WAN

La característica redireccionamiento de WAN es una función más avanzada. Al utilizar dicha característica, se configura un enlace principal y uno alternativo. En el caso de que el enlace principal diera un error, se arrancaría el enlace alternativo. Los protocolos de direccionamiento (por ejemplo, RIP u OSPF) detectan la disponibilidad del nuevo enlace y ajustan las rutas utilizadas para reenviar paquetes.

Para el redireccionamiento de WAN:

- El enlace principal y el alternativo están conectados.
- Se pueden configurar varios enlaces principales de forma que utilicen el mismo enlace alternativo.
- Se deben configurar las definiciones de protocolos para el enlace alternativo.
- El enlace principal puede ser un enlace para el que se puedan configurar protocolos direccionables (por ejemplo, IP o IPX). Por ejemplo, el enlace principal puede ser una interfaz LAN, PPP, Frame Relay o una interfaz X.25 serie, o un circuito de marcación PPP o Frame Relay. Los siguientes tipos de interfaz no pueden ser enlaces principales: interfaces SDLC serie, interfaces SRLY serie y redes base como V.25bis y RDSI.
- El enlace alternativo puede ser un enlace para el que se puedan configurar protocolos direccionables (por ejemplo IP o IPX) , y el tipo de enlace de datos del enlace alternativo debe ser distinto del del enlace principal. Por ejemplo, el enlace alternativo puede ser una interfaz LAN, PPP, Frame Relay, o una interfaz X.25 serie, o un circuito de datos PPP o Frame Relay. Los siguientes tipos de interfaz no pueden ser enlaces alternativos: interfaces SDLC serie, interfaces SRLY serie, y redes base como V.25bis y RDSI.
- Si el enlace principal es un circuito de marcación, no puede ser un circuito de marcación a petición. Para configurar un circuito de marcación de forma que no sea un circuito de marcación a petición, debe configurarlo con el mandato **set idle 0** en el indicador de marcación `Circuit Config>`. Para obtener más información, consulte el apartado “Configuración y supervisión de circuitos de marcación”, en el *Software de Access Integration Services Guía del usuario.*

  Los circuitos de marcación I.430, I.431 y T1/E1 canalizado, son implícitamente fijos y, por lo tanto, pueden utilizarse como WRS principal.

  Nota: Los circuitos de marcación I.430/I.431 y T1/E1 canalizado, pueden utilizarse como WRS principal sin tener que configurarlos explícitamente.

- El enlace alternativo no puede ser un circuito de marcación a petición (debe configurar **set idle 0** para el circuito de marcación).
- Se debe habilitar la característica WRS ejecutando el mandato **enable wrs**.
- Se debe habilitar la conexión entre los enlaces principal y alternativo ejecutando el mandato **enable alternate-circuit**.
- Opcionalmente se pueden configurar las horas de estabilización, las horas de estabilización de rutas y las horas de inicio y fin de reversión, para controlar la reversión al enlace principal.
- Si el enlace alternativo es X.25, debería utilizar el mandato **national-personality set disconnect-procedure active** al configurar la interfaz

X.25 del direccionador que tiene la característica de redireccionamiento de WAN habilitada, y el mandato **national-personality set disconnect-procedure passive** al configurar la interfaz X.25 del otro direccionador.

marcación por desbordamiento

La característica marcación por desbordamiento es parecida a la de redireccionamiento de WAN, con la diferencia de que no es necesario que el enlace principal dé un error para arrancar el enlace alternativo. En cambio, se supervisa la utilización del enlace principal y, si se supera un umbral, se arranca el enlace alternativo. Además, no se cargan todos los protocolos en el enlace alternativo. En el enlace alternativo sólo se carga IP y el resto de protocolos siguen utilizando el enlance principal, a menos que se desactive.

Si el enlace principal se desactiva, el redireccionamiento de WAN toma el control y todos los protocolos configurados para la interfaz alternativa pueden empezar a detectar y utilizar rutas de la interfaz alternativa.

Para la marcación por desbordamiento:

- La marcación por desbordamiento utiliza la conexión entre los enlaces principal y alternativo de una conexión de un redireccionamiento de WAN.
- Se debe configurar una conexión de un redireccionamiento de WAN para poder utilizar la marcación por desbordamiento y se aplican todas las restricciones de la configuración del redireccionamiento de WAN.
- El enlace principal de una conexión de un redireccionamiento de WAN que utilizará la marcación por desbordamiento, debe ser Frame Relay.
- Para utilizar la marcación por desbordamiento, se debe utilizar el protocolo de direccionamiento OSPF.
- Se debe utilizar el mandato **enable dial-on-overflow** para configurar los umbrales de aumentar y de reducir, el intervalo de supervisión del ancho de banda y el tiempo mínimo que el enlace alternativo estará activo.
- Las horas de estabilización, de estabilización de rutas y de inicio y fin de reversión, no afectan al funcionamiento de la marcación por desbordamiento.

Para obtener más información sobre el redireccionamiento de WAN, consulte Capítulo 7, “La característica de redireccionamiento de WAN” en la página 97.

Antes de empezar

Antes de configurar la restauración de WAN, debe tener lo siguiente:

1. Una interfaz serie principal (una línea cedida) configurada para PPP. Para el direccionador se puede utilizar cualquier interfaz serie.
2. Una interfaz con los circuitos de marcación asociados configurada para el direccionador. Como red base, se puede utilizar una interfaz RDSI o V.25bis.
3. Un circuito de marcación secundario configurado para establecer conexión si la interfaz principal se desactiva. Para configurar un circuito de marcación para que haga esto, establezca el temporizador de desocupado a cero ejecutando el mandato **set idle**, en el indicador de marcación `Circuit Config>`. Este mandato evita que el circuito de marcación sea un circuito de marcación a petición.
4. Un circuito de marcación secundario en un extremo del enlace, configurado solamente para enviar llamadas. Ejecute el mandato **set calls outbound** en el indicador de marcación `Circuit Config>` .

Nota: No configure direcciones de protocolos para la interfaz secundaria. Cuando el enlace secundario (circuito de marcación) está activo, utilizará las asignaciones de protocolos de la interfaz principal.

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

Procedimiento de configuración de la restauración de WAN

En este apartado se describen los pasos necesarios para configurar la restauración de WAN. Antes de empezar, ejecute el mandato **list device** en el indicador `Config>`, para obtener una lista de los números de interfaz de los distintos dispositivos.

Para configurar la restauración de WAN en el direccionador, siga los pasos siguientes :

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

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

2. Asigne un circuito de marcación secundario a la interfaz principal. Este es el circuito de reserva de la interfaz principal. 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 se acaba de añadir. Por ejemplo:

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

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

```
WRS Config>enable wrs
```

5. Reinicie el direccionador para que entren en vigor los cambios hechos a la configuración.

Configuración del circuito de marcación secundario

Para configurar un circuito de marcación:

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

```
Config> list device
```

   Si no se obtiene ninguna interfaz PPP de circuito de marcación, añada una interfaz de circuito de marcación escribiendo:

```
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 desde el indicador `Config>` la interfaz secundaria (circuito de marcación), de forma que su tipo de enlace de datos sea el mismo que el de la interfaz principal (PPP):

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

3. Acceda al indicador de configuración del circuito de marcación (`Circuit Config>`) escribiendo **network** *número-interfaz*.

   ```
   Config>
   network 3
   ```

4. Seleccione la interfaz de la red base del circuito de marcación. La red base puede ser V.25bis, ó RDSI.

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

5. Establezca el temporizador de desocupado a 0 (0=fijo) así:

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

6. Establezca uno de los extremos de la conexión de reserva para que reciba las llamadas (por ejemplo, el direccionador A):

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

7. Establezca el otro extremo de la conexión de reserva para que inicie las llamadas (por ejemplo, el direccionador B):

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

Notas:

1. No utilice el mandato **set calls both**. Al establecer los circuitos individualmente se evitarán colisiones entre intentos de conexión de entrada y de salida.
2. No configure ninguna dirección de reenvío (por ejemplo, IP, IPX, etc.) para el circuito de marcación. Las asignaciones de protocolos de la interfaz principal se utilizarán en la interfaz secundaria (circuito de marcación) cuando esté activa.
3. Para obtener instrucciones sobre cómo configurar la interfaz RDSI, consulte el apartado “Utilización de la interfaz RDSI”, en el *Software de Access Integration Services Guía del usuario.*
4. Para obtener instrucciones sobre la configuración de la interfaz V.25bis, consulte el apartado “Utilización de la interfaz V.25bis”, en el *Software de Access Integration Services Guía del usuario.*

Utilización de la restauración de WAN

Capítulo 6. Configuración y supervisión de la restauración de WAN

En este capítulo se describen los mandatos de configuración y de funcionamiento de la restauración de WAN. Consta de los apartados siguientes:

- "Acceso al proceso de supervisión de interfaces de la restauración de WAN" en la página 85
- "Mandatos de supervisión de la restauración de WAN" en la página 85

Nota: Consulte el apartado "Configuración y supervisión de circuitos de marcación", del *Software de Access Integration Services Guía del usuario* para obtener más información sobre la configuración de circuitos de marcación. Un circuito de marcación puede utilizarse como interfaz si se configura el redireccionamiento de WAN.

Mandatos de configuración de la restauración de WAN, del redireccionamiento de WAN y de la marcación por desbordamiento

Los mandatos de configuración de la restauración de WAN le permiten crear o modificar la configuración de la interfaz de la restauración de WAN. En este apartado se ofrece un resumen de los mandatos de configuración de la restauración de WAN y, a continuación, se explican con más detalle.

La Tabla 8 lista los mandatos de configuración de la restauración de WAN y sus funciones. Entre los mandatos en el indicador `WRS Config>`. Para acceder al indicador `WRS Config>`, escriba **feature wrs** en el indicador `Config>`.

Tabla 8. Resumen de los mandatos de configuración de la restauración de WAN

Mandato	Función
? (Ayuda)	Visualiza todos los mandatos disponibles para este nivel de mandato, o lista las opciones de mandatos específicos (si es que están disponibles). Consulte "Obtención de ayuda" en la página xxv.
Add	Añade una correlación de principal a secundario (para la restauración de WAN) o principal a alternativo (para el redireccionamiento de WAN).
Disable	Inhabilita WRS, o una correlación de un único circuito secundario o alternativo.
Enable	Habilita WRS, o una correlación de un único circuito secundario o alternativo.
List	Muestra la configuración actual de la restauración de WAN.
Remove	Elimina una correlación principal a secundario o principal a alternativo, creada previamente con el mandato add.
Set	Establece los valores de los temporizadores de estabilización, estabilización de ruta y hora de reversión.
Exit	Hace volver al nivel de mandato anterior. Consulte "Salida de un entorno de nivel inferior" en la página xxv.

Add

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

Sintaxis:

add alternate-circuit
secondary-circuit

alternate-circuit

El mandato **add alternate-circuit** enlaza una interfaz alternativa con una interfaz principal, para los propósitos del redireccionamiento de WAN. Se pueden asignar varias interfaces principales a una sola interfaz alternativa. El tipo del enlace alternativo no tiene por que ser el mismo que el del enlace principal (por ejemplo, el tipo del enlace alternativo puede ser un circuito PPP de marcación y el del enlace principal puede ser una línea Frame Relay cedida).

Ejemplo:

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

Alternate interface number

Es el número de la interfaz que se ha asignado antes como interfaz alternativa. Como interfaz alternativa se puede elegir entre una interfaz LAN, PPP, Frame Relay, una interfaz X.25 serie, o un circuito PPP de marcación o Frame Relay. El valor por omisión es 0.

Primary interface number

Es el número de interfaz de la interfaz principal que se ha asignado al añadir el dispositivo. Una interfaz principal puede ser una interfaz LAN, PPP, Frame Relay, o una interfaz X.25 serie, o un circuito PPP de marcación o Frame Relay, que se haya definido previamente. El valor por omisión es 0.

secondary-circuit

sl mandato **add secondary-circuit** enlaza una interfaz secundaria con una interfaz principal, para los propósitos de la restauración de WAN. Ambas interfaces deben haberse configurado previamente. Se puede asignar una sola interfaz secundaria a la interfaz principal 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 del circuito de marcación asignado previamente al añadir el dispositivo a la interfaz secundaria. Cualquier circuito PPP de marcación 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 principal asignado previamente al añadir el dispositivo. Una interfaz principal puede ser cualquier línea alquilada definida previamente y que ejecute PPP. El valor por omisión es 0.

Disable

Utilice el mandato **disable** para inhabilitar la función de restauración de WAN, o para inhabilitar una conexión entre los enlaces principal y secundario para la restauración de WAN, o para inhabilitar una conexión entre los enlaces principal y alternativo para el redireccionamiento de WAN, o para inhabilitar la marcación por desbordamiento para una conexión entre los enlaces principal y alternativo.

Sintaxis:

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

alternate-circuit *número-interfaz*
Inhabilita la conexión entre los enlaces principal y alternativo para el redireccionamiento de WAN.

Ejemplo:

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

Alternate interface number
Es el numero de la interfaz alternativa previamente configurada con el mandato **add alternate-circuit**. El valor por omisión es 0.

dial-on-overflow *número-interfaz-alternativa*
Inhabilita la marcación por desbordamiento para todas las conexiones entre los enlaces principal y alternativo que utilizan un enlace alternativo determinado.

Ejemplo:

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

Alternate interface number
Es el numero de la interfaz alternativa previamente configurada con el mandato **add alternate-circuit**. El valor por omisión es 0.

secondary-circuit *número-interfaz*
No permite que una interfaz secundaria restaure una interfaz principal asociada concreta, hasta que se ejecute el próximo mandato **enable secondary-circuit** en la consola WRS. Ambas interfaces deben haber sido previamente configuradas y enlazadas en la configuración WRS.

Ejemplo:

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

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

wrs Inhabilita globalmente en el direccionador la característica de restauración de WAN. Esto significa que también se inhabilitan las características de redireccionamiento de WAN y de marcación por desbordamiento.

Enable

Utilice el mandato **enable** para habilitar la restauración de WAN, o para habilitar una conexión entre los enlaces principal y secundario para la restauración de WAN, o para habilitar una conexión entre los enlaces principal y alternativo para el redireccionamiento de WAN, o para habilitar la marcación por desbordamiento para una conexión entre los enlaces principal y alternativo.

Sintaxis:

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

alternate-circuit *número-interfaz*
Habilita un circuito alternativo

Ejemplo:

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

Alternate interface number
Es el numero de la interfaz alternativa previamente configurada con el mandato **add alternate-circuit**. El valor por omisión es 0.

dial-on-overflow
Habilita la marcación por desbordamiento y permite establecer parámetros para controlar el funcionamiento de la marcación por 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 principal para la que se está habilitando la marcación por desbordamiento. El valor por omisión es 0.

add-threshold
Determina si se cargará una interfaz alternativa para obtener ancho de banda adicional. Este valor se expresa como un porcentaje de la velocidad de la línea configurada para la interfaz principal. El valor por omisión es el 90%.

drop-threshold
Determina cuando dejará de ser necesaria una interfaz alternativa que ofrece ancho de banda adicional. Este valor se expresa como un porcentaje de la velocidad de la línea configurada para la interfaz principal. El valor por omisión es el 60%.

bandwidth monitoring interval
Determina con qué frecuencia se supervisará el ancho de banda de la interfaz principal para comprobar los valores *umbral de aumentar* y *umbral de reducir*. El valor por omisión es 15 segundos.

Minimum time to keep alternate up
Este período de tiempo debe ser lo suficientemente largo como para permitir que el direccionador establezca una ruta nueva cuando el tráfico IP del direccionador local se redirecciona a la interfaz alternativa. El valor por omisión es 5 minutos.

secondary-circuit *número-interfaz*
Habilita la restauración de un enlace principal para 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 previamente configurada con el mandato **add secondary-circuit**. El valor por omisión es 0.

wrs Habilita en el direccionador la función de la restauración de WAN. Esto significa que si están configuradas las funciones de redireccionamiento de WAN y marcación por desbordamiento, también se habilitarán.

List

Utilice el mandato **list** para ver la información de configuración global de la función y la información de configuración de la marcación por desbordamiento, de las conexiones entre el enlace principal y el secundario para la restauración de WAN y de las conexiones entre el enlace principal y el alternativo para el redireccionamiento de WAN.

Sintaxis:

list

Ejemplo:

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

                                                 Secondary
   Primary Interface       Secondary Interface   Enabled
-----------------------  -----------------------  --------
 4 - WAN PPP             7 - PPP Dial Circuit       No
                                        Alt.     1st  Subseq TOD Revert Back  Stab
Primary Interface  Alternate Interface  Enabled  Stab  Stab  Start    Stop
-----------------  -----------------------  -------  ----  ----  --------  ------- ----

 1 - WAN Frame Re   2 - WAN Frame Relay      Yes    dflt  dflt  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 eliminar la correlación entre una interfaz alternativa o secundaria (de reserva) y la interfaz principal.

Sintaxis:

remove alternate-circuit
secondary-circuit

alternate-circuit *número-interfaz-alternativa número-interfaz-principal*
Elimina la correlación entre una interfaz alternativa (de reserva) y la interfaz principal para el redireccionamiento de WAN. Ambas interfaces deben haber sido previamente asignadas y enlazadas con el mandato **add alternate-circuit**.

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

número-interfaz-principal
Es el número de interfaz de la interfaz principal enlazada previamente a la interfaz alternativa que se está eliminando. El valor por omisión es 0.

Ejemplo:

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

secondary-circuit *número-interfaz-secundaria número-interfaz-principal*
Elimina la correlación entre una interfaz secundaria (de reserva y la interfaz principal para la restauración de WAN. Ambas interfaces deben haber sido previamente asignadas y enlazadas con el mandato **add secondary-circuit**.

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

número-interfaz-principal
Es el número de interfaz de la interfaz principal enlazada previamente a la interfaz secundaria que se está eliminando. 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 establecer los parámetros del 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 establecer los valores por omisión que utilizarán los enlaces que no tienen configuradas horas de estabilización y de primera estabilización.

first-stabilization

Establece el valor por omisión de la primera estabilización que utilizarán los enlaces que no tengan configurada una hora de primera estabilización.

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

stabilization

Establece el valor por omisión de estabilización que utilizarán los enlaces que no tengan configurada una hora de estabilización.

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

first-stabilization

Establece el número de segundos que se esperará el direccionador durante la inicialización antes de que el direccionamiento del enlace principal, si éste no está activo, se pase al enlace alternativo.

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 de la interfaz principal para la que se está estableciendo la primera estabilización. El valor por omisión es 0.

First primary stabilization time

Hora de estabilización de esta interfaz principal. El valor por omisión es 1.

routing-stabilization

Establece el valor de estabilización de ruta. Este parámetro define el número de segundos que, tanto el enlace principal como el enlace alternativo, permanecerán activos después de detectar que el enlace principal está activo y que el tiempo de estabilización, si se ha definido, se ha agotado. La hora de estabilización de ruta está definida de forma que los protocolos de direccionamiento, como OSPF o RIP, tengan tiempo suficiente para reconocer la disponibilidad de una ruta nueva. Sin el temporizador de estabilización de ruta, el tráfico podría ser interrumpido durante varios segundos, en el intervalo de tiempo que transcurre desde que se inhabilita la ruta alternativa hasta que se descubre la ruta principal.

Si el enlace alternativo estaba activo antes de la redirección, éste sigue activo y se hace caso omiso del temporizador de estabilización de ruta. Si el enlace alternativo se desactivó antes o durante la redirección, el enlace alternativo sigue desactivado y se hace caso omiso del temporizador de estabilización de ruta y del 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: de 1 a 3600 segundos

Valor por omisión: 0

stabilization

Establece el número de segundos que deben transcurrir después de que se detecte por primera vez que el enlace principal está activo y antes de que empiece el proceso de reinicialización del direccionamiento en el enlace principal. Cuando se agota el tiempo de estabilización, se desactivará el enlace alternativo, a menos que se haya configurado el temporizador de estabilización de ruta. El temporizador de estabilización de ruta empezará a contar tan pronto como se agote el tiempo de estabilización y mantendrá activos los enlaces principal y alternativo el tiempo suficiente para mantener el tráfico del enlace alternativo hasta que los protocolos de direccionamiento, como OSPF y RIP, vuelvan a establecer la ruta en el enlace principal.

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 de la interfaz principal para la que se está definiendo la estabilización. El valor por omisión es 0.

Primary stabilization time

La hora de estabilización de la interfaz principal. El valor por omisión es 1.

start-time-of-day-revert-back

La hora del día en que el direccionador puede revertir a la ruta principal. El direccionador puede revertir a la interfaz principal en cualquier momento entre la hora de inicio y de fin de reversión. Sólo se revertirá a la interfaz principal si ésta está activa 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 de la interfaz principal para la que se está estableciendo la primera estabilización. El valor por omisión es 0.

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

Este tiempo señala la hora de inicio de la ventana de reversión. El direccionador puede revertir a la interfaz principal en cualquier momento entre la hora de inicio y de fin de reversión. Sólo se revertirá a la interfaz principal si ésta está activa y se cumplen los parámetros de estabilización. El valor por omisión es 1.

stop-time-of-day-revert-back

Este tiempo señala la hora final de la ventana de reversión. El direccionador puede revertir a la interfaz principal en cualquier momento entre la hora de inicio y de fin de reversión. Sólo se revertirá a la interfaz

principal si ésta está activa 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 de la interfaz principal para la que se está estableciendo la primera estabilización. El valor por omisión es 0.

Time-of-day-revert-back-window stop
Este tiempo señala la hora final de la ventana de reversión. El direccionador puede revertir a la interfaz principal en cualquier momento entre la hora de inicio y de fin de reversión. Sólo se revertirá a la interfaz principal si ésta está activa y se cumplen los parámetros de estabilización. El valor por omisión es 1.

Acceso al proceso de supervisión de interfaces de la restauración de WAN

Para acceder al proceso de supervisión de interfaces de la restauración de WAN, escriba el mandato siguiente 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 las conexiones entre los enlaces principal y secundario de la restauración de WAN, de las conexiones entre los enlaces principal y alternativo del redireccionamiento de WAN y de la marcación por desbordamiento. Las modificaciones del estado de funcionamiento de la restauración de WAN, del redireccionamiento de WAN y de la marcación por desbordamiento hechas desde la interfaz de supervisión, no tendrán efecto después de reinicializar el direccionador.

Acceda al indicador WRS escribiendo **feature wrs** en el indicador GWCON (+). La Tabla 9 muestra una lista de los mandatos de WRS y sus funciones, y en los apartados siguientes se explican con más detalle.

Tabla 9 (Página 1 de 2). Mandatos de supervisión de la restauración de WAN

Mandato	Función
? (Ayuda)	Visualiza todos los mandatos disponibles para este nivel de mandato, o lista las opciones de mandatos específicos (si es que están disponibles). Consulte “Obtención de ayuda” en la página xxv.
Clear	Borra las estadísticas de supervisión que se muestran con el mandato **list**.
Disable	Inhabilita el WRS, o un enlace secundario o alternativo individuales, o la marcación por desbordamiento.
Enable	Habilita el WRS, o un enlace secundario o alternativo individuales, o la marcación por desbordamiento.
List	Muestra la información de supervisión de uno o todos los circuitos alternativos o secundarios.

Tabla 9 (Página 2 de 2). Mandatos de supervisión de la restauración de WAN

Mandato	Función
Set	Establece los valores de los temporizadores de estabilización, estabilización de ruta y hora de reversión.
Exit	Hace volver al nivel de mandato anterior. Consulte “Salida de un entorno de nivel inferior” en la página xxv.

Clear

Utilice el mandato **clear** para borrar las estadísticas de la restauración de WAN, redireccionamiento de WAN y marcación por desbordamiento, que se muestran al ejecutar el mandato **list**.

Sintaxis:

clear

Nota: Este mandato borra el *Período de restauración más largo*, pero no borra el *Período de restauración más reciente*. En el ejemplo del mandato **list** puede verse una pantalla de ejemplo.

Disable

Utilice el mandato **disable** para inhabilitar totalmente la característica restauración de WAN, inhabilitar la restauración de una interfaz principal determinada a partir de su interfaz secundaria asociada, inhabilitar una interfaz alternativa, o inhabilitar la marcación por desbordamiento.

Sintaxis:

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

alternate-circuit

Inhabilita una conexión entre los enlaces principal y alternativo para el redireccionamiento de WAN. Pueden haber varias conexiones que utilicen el mismo enlace alternativo. Este mandato inhabilita todas las conexiones 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 por desbordamiento para la conexión entre los enlaces principal y alternativo, sin cambiar el estado habilitado o inhabilitado del redireccionamiento de WAN para esta conexión. Si la marcación por desbordamiento está direccionando activamente, se interrumpirá cuando termine el próximo intervalo de supervisión.

secondary-circuit

Inhabilita la restauración de una interfaz principal concreta por parte de su interfaz secundaria asociada hasta que se ejecute el próximo mandato

restart, **reload** o **enable secondary-circuit**. Ambas interfaces deben haber sido previamente configuradas y enlazadas en la configuración WRS.

Normalmente, en **talk 5** (GWCON), el mandato **disable** hace que la interfaz se inactive y permanezca inactiva. Sin embargo, esto no es cierto para la restauración de WAN. El mandato **disable** aplicado a la interfaz secundaria, no inhabilita la propia interfaz. Sólo inhabilita la llamada actual (o sea, hace que las llamadas activas se desconecten). Para inhabilitar la utilización del circuito secundario, deberá ejecutar el mandato **disable secondary-circuit** en el indicador de supervisión de la restauración de WAN e inhabilitar la interfaz secundaria en el indicador GWCON de mayor nivel.**Ejemplo:**

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

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

wrs Si se inhabilita WRS, se inhabilita en el direccionador la restauración de WAN, el redireccionamiento de WAN y la marcación por desbordamiento hasta la próxima ejecución del mandato **restart**, **reload** o **enable WRS**.

Enable

Utilice el mandato **enable** para habilitar la interfaz de la restauración de WAN, habilitar la restauración de un enlace principal a partir de un circuito secundario, habilitar un circuito alternativo, o habilitar la marcación por desbordamiento.

Sintaxis:

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

alternate-circuit
Habilita las conexiones entre los enlaces principal y alternativo para el redireccionamiento de WAN, para todas las conexiones que utilicen el enlace 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 por desbordamiento y permite establecer parámetros para controlar la marcación por desbordamiento. Opcionalmente, permite que el protocolo IP se conecte inmediatamente con el circuito alternativo, como si se hubiera superado el umbral de aumentar.

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 principal para el enlace secundario indicado.

Ejemplo:

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

Secondary interface number

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

wrs Habilita en el direccionador la función restauración de WAN. Para que funcione la restauración de WAN, el redireccionamiento de WAN o la marcación por desbordamiento, es necesario habilitar está función.

Set

Utilice el mandato **set** para establecer los parámetros del 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 establecer los valores por omisión que utilizarán los enlaces que no tienen configuradas horas de estabilización y de primera estabilización.

Ejemplo:

```
WRS Config>set default ?
FIRST-STABILIZATION
STABILIZATION
```

first-stabilization

Establece el valor por omisión de la primera estabilización que utilizarán los enlaces que no tengan configurada una hora de primera estabilización.

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

stabilization

Establece el valor por omisión de estabilización que utilizarán los enlaces que no tengan configurada una hora de estabilización.

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

first-stabilization

Establece el número de segundos que se esperará el direccionador durante la inicialización antes de que el direccionamiento del enlace principal, si no está activo, pase al enlace alternativo.

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 de la interfaz principal para la que se está estableciendo la primera estabilización. El valor por omisión es 0.

First primary stabilization time

Hora de estabilización de esta interfaz principal. El valor por omisión es 1.

routing-stabilization

Establece el valor de estabilización de ruta. Este parámetro define el número de segundos que, tanto el enlace principal como el enlace alternativo, permanecerán activos después de detectar que el enlace principal está activo y que el tiempo de estabilización, si se ha definido, se ha agotado. La hora de estabilización de ruta está definida de forma que los protocolos de direccionamiento, como OSPF o RIP, tengan tiempo suficiente para reconocer la disponibilidad de una ruta nueva. Sin el temporizador de estabilización de ruta, el tráfico podría ser interrumpido durante varios segundos, en el intervalo de tiempo que transcurre desde que se inhabilita la ruta alternativa hasta que se descubre la ruta principal.

Si el enlace alternativo estaba activo antes de la redirección, éste sigue activo y se hace caso omiso del temporizador de estabilización de ruta. Si el enlace alternativo se desactivó antes o durante la redirección, el enlace alternativo sigue desactivado y se hace caso omiso del temporizador de estabilización de ruta y del 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 configuradas en el direccionador

Valor por omisión: 0

Routing-stabilization timer

Valores válidos: de 1 a 3600 segundos

Valor por omisión: 0

stabilization

Establece el número de segundos que deben transcurrir después de que se detecte por primera vez que el enlace principal está activo y antes de que empiece el proceso de reinicialización del direccionamiento en el enlace principal. Cuando se agota el tiempo de estabilización, se desactivará el enlace alternativo, a menos que se haya configurado el temporizador de estabilización de ruta. El temporizador de estabilización de ruta empezará a contar tan pronto como se agote el tiempo de estabilización y mantendrá

activos los enlaces principal y alternativo el tiempo suficiente para mantener el tráfico del enlace alternativo hasta que los protocolos de direccionamiento, como OSPF y RIP, vuelvan a establecer la ruta en el enlace principal.

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 de la interfaz principal para la que se está definiendo la estabilización. El valor por omisión es 0.

Primary stabilization time
La hora de estabilización de la interfaz principal. El valor por omisión es 1.

start-time-of-day-revert-back
Establece la hora del día en que el direccionador podrá revertir a la ruta principal. El direccionador puede revertir a la interfaz principal en cualquier momento entre la hora de inicio y de fin de reversión. Sólo se revertirá a la interfaz principal si ésta está activa 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 de la interfaz principal para la que se está estableciendo la primera estabilización. El valor por omisión es 0.

Time-of-day-revert-back-window start
Este tiempo señala la hora de inicio de la ventana de reversión. El direccionador puede revertir a la interfaz principal en cualquier momento entre la hora de inicio y de fin de reversión. Sólo se revertirá a la interfaz principal si ésta está activa y se cumplen los parámetros de estabilización. El valor por omisión es 1.

stop-time-of-day-revert-back
Este tiempo señala la hora final de la ventana de reversión. El direccionador puede revertir a la interfaz principal en cualquier momento entre la hora de inicio y de fin de reversión. Sólo se revertirá a la interfaz principal si ésta está activa 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 de la interfaz principal para la que se está estableciendo la primera estabilización. El valor por omisión es 0.

Time-of-day-revert-back-window stop
Este tiempo señala la hora final de la ventana de reversión. El direccionador puede revertir a la interfaz principal en cualquier momento entre la hora de inicio y de fin de reversión. Sólo se revertirá a la interfaz principal si ésta está activa y se cumplen los parámetros de estabilización. El valor por omisión es 1.

List

Utilice el mandato **list** para ver la información de supervisión de una o de todas las conexión entre los enlaces principal y secundario de la restauración de WAN, o de una o todas las conexiones entre los enlaces principal y alternativo del redireccionamiento de WAN.

Sintaxis:

list all
alternate-circuit
secondary-circuit
summary

all Proporciona información resumida, seguida por la información específica de 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

                                Re-route/ Re-route/         Recent
   Primary       Alternate    Overflow  Overflow     Reroute/Overflow
Net Interface  Net Interface  Enabled    Active          Duration
-------------  -------------  --------  --------   --------------------
  1   FR/0       2   FR/1     Yes/Yes    No /No     00:00:56/ 00:05:00
```

Total restoral attempts
Número de veces que el enlace principal ha dado un error, haciendo que el direccionador intente activar un enlace secundario.

Completions
Número de intentos satisfactorios de restauración, en los que se ha activado y utilizado el enlace secundario.

Total packets forwarded
Número total de paquetes reenviados por la interfaz secundaria. Es la suma del número de paquetes reenviados en ambos sentidos, y el valor se acumulará en cada restauración satisfactoria, hasta que se ejecute el mandato de reiniciar o borrar las estadísticas de restauración.

Longest Completed Restoral Period
Este campo muestra en horas, minutos y segundos, el tiempo más largo que ha estado en funcionamiento la función de restauración, sin contar el tiempo de funcionamiento actual.

Total Overflow Attempts
Número de intentos debidos a un desbordamiento.

Completions
Número de intentos satisfactorios debidos a un desbordamiento, en los que se ha activado y utilizado el enlace secundario.

Longest Completed Overflow Period
Muestra en horas, minutos y segundos, el tiempo más largo que ha estado en funcionamiento la función de marcación por desbordamiento, sin contar el tiempo de funcionamiento actual.

Primary Net Interface
La interfaz que está siendo respaldada por la interfaz secundaria asociada.

Secondary Net Interface
El circuito de marcación que se está utilizando para respaldar la interfaz principal asociada.

Restoral Enabled
Indica que la restauración de esta interfaz principal está actualmente habilitada.

Restoral Active
Indica si la restauración está activa o no.

Current/Longest Duration
Indica en horas, minutos y segundos, el tiempo actual y el más largo de funcionamiento de la interfaz de red secundaria.

Primary Net Interface
La interfaz que está siendo respaldada por la interfaz alternativa asociada.

Alternate Net Interface
La interfaz alternativa que se está utilizando para respaldar la interfaz principal asociada.

Re-route/Overflow Enabled
Indica si las funciones de redireccionamiento y de desbordamiento están habilitadas o no.

Re-route/Overflow Active
Indica si las funciones de redireccionamiento y de desbordamiento están activas o no.

Recent Re-route Overflow Duration
Indica, en horas, minutos y segundos, el tiempo más reciente en que la interfaz de red alternativa ha sido redireccionada o desbordada.

Alternate-circuit
Proporciona valores totales para un circuito alternativo. Permite que el operador encargado de la supervisión, recupere el estado del redireccionamiento de WAN y las estadísticas asociadas para cada interfaz alternativa y sus interfaces principales asociadas.

Ejemplo:

```
WRS>li 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 que esta siendo respaldada por la interfaz alternativa asociada.

Alternate Interface
El circuito de marcación que se está utilizando para respaldar la interfaz principal asociada.

Reroute Enabled
Indica si el redireccionamiento de esta interfaz principal está actualmente habilitado.

Overflow Enabled
Indica si el desbordamiento de esta interfaz principal está actualmente habilitado.

Primary first stabilization
Número de segundos que se esperará el direccionador durante la inicialización antes de que el direccionamiento del enlace principal, si éste no está activo, se pase al enlace alternativo.

First stabilization
Número de segundos que deben transcurrir después de que se detecte por primera vez que el enlace principal está activo y antes de que se devuelva el direccionamiento del enlace alternativo al principal. El direccionamiento continuará utilizando el enlace alternativo hasta que el enlace principal permanezca activo durante este número de segundos.

Routing stabilization
Número de segundos que deben transcurrir después de que se devuelva el direccionamiento al enlace principal y antes de que se desactive el enlace alternativo. Durante este tiempo, ambos enlaces permanecerán activos. Este intervalo permite que protocolos de direccionamiento, como OSPF y RIP, tengan tiempo de reconocer que se dispone de una ruta a través de la interfaz principal.

Time-of-day revert back
Hora del día en que el direccionador puede revertir a la ruta principal. El direccionador puede revertir a la interfaz principal en cualquier momento entre la hora de inicio y de fin de reversión. Sólo se revertirá a la interfaz principal si ésta está activa y se cumplen los parámetros de estabilización. El valor por omisión es 0.

Restored times
Número de intentos de redireccionar la interfaz principal.

Overflow times
Número de intentos de marcación por desbordamiento.

secondary-circuit
Proporciona valores totales para cada circuito secundario. Permite que el operador encargado de la supervisión, recupere el estado de la restauración de WAN y las estadísticas asociadas para cada interfaz secundaria y sus interfaces principales asociadas.

Ejemplo:

Configuración de la restauración de WAN

```
list secondary-circuit
Secondary interface number  [0]? 1

                                                    Secondary
Primary Interface          Secondary Interface      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
La interfaz que está siendo respaldada por la interfaz secundaria asociada.

Secondary Interface
El circuito de marcación que se está utilizando para respaldar la interfaz principal asociada.

Secondary Enabled
Indica si la restauración de esta interfaz principal está actualmente habilitada.

Router Primary Interface State
Indica que el estado de la interfaz principal es uno de estos:

Up - Indica que el enlace está activo.

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 que hay un problema de hardware.

Router Secondary Interface State
Indica que el estado de la interfaz secundaria asociada es uno de estos:

Up - Indica que el enlace está activo.

Down - Indica que el enlace está desactivado. También sucede cuando la red básica del enlace secundario se inhabilita desde el indicador `Config>` o desde la consola del operador.

Available - Indica que el enlace está en modalidad de espera.

Testing - Indica que el enlace está en proceso de establecer una conexión.

Restoral Statistics:

Primary Restoral Attempts
Número de veces que el enlace principal ha dado un error, 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
Indica durante cuánto tiempo ha estado activo el enlace secundario, la última vez que se utilizó o durante la restauración actual.

summary

Proporciona valores 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 el enlace principal ha dado un error, haciendo que el direccionador intente activar un enlace secundario.

Completions

Número de intentos satisfactorios de restauración en los que se ha activado y utilizado el enlace secundario.

Total packets forwarded

Número total de paquetes reenviados por la interfaz secundaria. Es la suma del número de paquetes reenviados en ambos sentidos. El valor se va acumulando cada período de restauración, hasta que se ejecute el mandato de reiniciar o borrar las estadísticas de restauración.

Longest restoral period

Este campo muestra en horas, minutos y segundos, el tiempo más largo que ha estado en funcionamiento la función de restauración, sin contar el tiempo de funcionamiento actual.

Primary Interface and State

La interfaz que está siendo respaldada por la interfaz secundaria asociada. Los estados válidos son:

Up - Indica que el enlace está activo.

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 que hay un problema de hardware.

Secondary Interface and State

El circuito de marcación que se está utilizando para respaldar la interfaz principal asociada. Los estados válidos son:

Up - Indica que el enlace está activo.

Down - Indica que el enlace está desactivado. También sucede cuando la red básica del enlace secundario se inhabilita desde el indicador `Config>` o desde la consola del operador.

Testing - Indica que el enlace está en proceso de establecer una conexión.

Available - Indica que el enlace está en modalidad de espera.

Configuración de la restauración de WAN

Capítulo 7. La característica de redireccionamiento de WAN

En este capítulo se describe la característica de redireccionamiento de WAN. Consta de los apartados siguientes:

- "Visión general del redireccionamiento de WAN"
- "Configuración del redireccionamiento de WAN" en la página 99

Visión general del redireccionamiento de WAN

El redireccionamiento de WAN le permite configurar una ruta alternativa de forma que si un enlace principal da un error, el direccionador iniciará una conexión nueva con el destino a través de la ruta alternativa. En el apartado "Visión general de las características restauración de WAN, redireccionamiento de WAN y marcación por desbordamiento" en la página 71, se da una explicación del restablecimiento de WAN y de cómo trabajan juntos el redireccionamiento de WAN y la Marcación por desbordamiento.

El proceso de redireccionamiento de WAN implica:

1. Detectar el error del enlace principal
2. Pasar al enlace alternativo
3. Detectar la recuperación del enlace principal
4. Revertir al enlace principal

El enlace alternativo puede ser cualquier enlace para el que se puedan configurar protocolos direccionables (por ejemplo, IP o IPX), y el tipo de enlace de datos del enlace alternativo debe ser distinto al del enlace principal. Por ejemplo, el enlace alternativo puede ser una interfaz LAN, o una interfaz PPP, Frame Relay, o X.25 serie, o un circuito PPP o Frame Relay de marcación. Los siguientes tipos de interfaz no pueden ser enlaces alternativos: interfaces SDLC serie, interfaces SRLY serie, y redes base como V.25bis y RDSI.

Nota: Si los enlaces principal o alternativo son circuitos de marcación, éste no debe configurarse para marcación a petición. Utilice el mandato **set idle 0** en el indicador `Circuit Config>`, para configurar el circuito de marcación de forma que no pueda realizar marcación a petición. Para obtener más información, consulte el apartado "Configuración y supervisión de circuitos de marcación" en el *Software de Access Integration Services Guía del usuario.*

Configuración del redireccionamiento de WAN

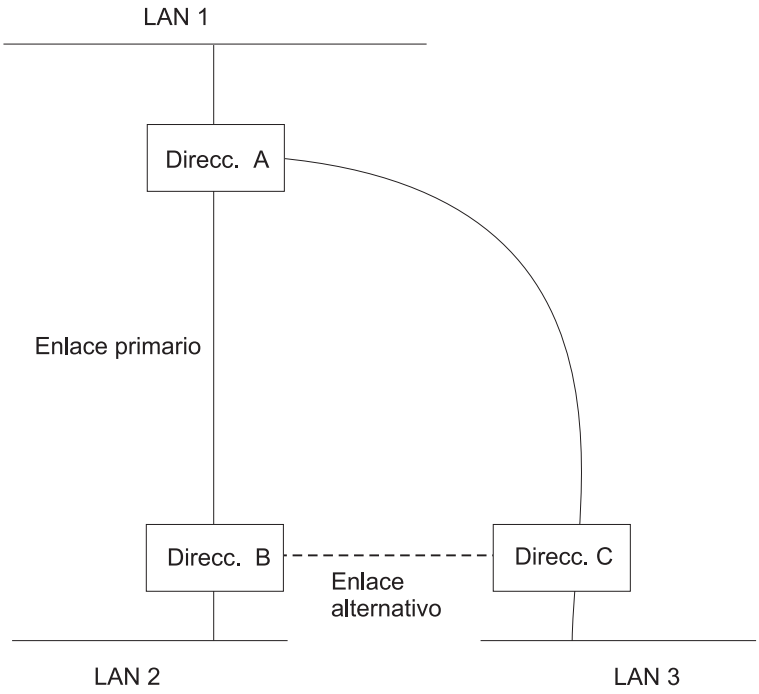


Figura 3. Redireccionamiento de WAN. Generalmente hay una conexión entre los direccionadores A y B y los direccionadores A y C. Si el enlace principal entre los direccionadores A y B da un error, el redireccionamiento de WAN establece un enlace alternativo entre los direccionadores B y C. De esta forma, los direccionadores A y B pueden comunicarse a través del direccionador C.

Marcación por desbordamiento

La marcación por desbordamiento le permite utilizar una interfaz alternativa para el tráfico IP cuando la tasa de tráfico del enlace principal alcanza un umbral determinado. Esto significa que la interfaz principal no tiene porqué estar desactivada antes de que el enlace alternativo se active. Cuando el tráfico de la interfaz principal alcanza el umbral especificado, el direccionador activa el enlace alternativo. Para utilizar la marcación por desbordamiento, debe configurarse el redireccionamiento de WAN y la interfaz principal debe ser Frame Relay. IP es el único protocolo que puede conmutar a una interfaz alternativa por marcación por desbordamiento. Además, si se utiliza la marcación por desbordamiento, debe utilizarse OSPF como protocolo IP de direccionamiento, en lugar de RIP.

Para obtener más información sobre la configuración de la marcación por desbordamiento, consulte el apartado “Mandatos de configuración de la restauración de WAN, del redireccionamiento de WAN y de la marcación por desbordamiento” en la página 77.

Supervisión del ancho de banda

Durante la configuración del redireccionamiento de WAN, puede especificarse un intervalo de supervisión del ancho de banda para la marcación por desbordamiento. Se supervisa la utilización del ancho de banda de recepción y trasmisión de la interfaz principal. Cuando el ancho de banda de la interfaz principal alcanza el umbral de *aumentar*, se emitirá una petición de redireccionamiento de WAN para activar la interfaz alternativa. Si el redireccionamiento de WAN logra activar la interfaz alternativa, IP deja de

direccionar por la interfaz principal y comienza a hacerlo por la interfaz alternativa.

Si el redireccionamiento de WAN no logra activar la ruta alternativa, intentará activar periódicamente la interfaz alternativa hasta que la utilización del ancho de banda de la interfaz principal caiga por debajo del umbral de *reducir*.

Cuando la utilización del ancho de banda de recepción y transmisión de la interfaz principal alcanza el umbral de *reducir* y se ha agotado el tiempo mínimo configurado que la interfaz alternativa estará activa, ésta se desactiva. Esto hace que IP deje de direccionar por la interfaz alternativa y empiece a utilizar la interfaz principal.

Los umbrales de aumentar y de reducir se especifican como un porcentaje de la velocidad configurada de la línea del enlace principal. La velocidad configurada de la línea no siempre coincide con la velocidad real del enlace. El volumen de tráfico del enlace en cada sentido se calcula por separado. Se cruza el umbral si el tráfico en cualquiera de los dos sentidos es mayor que el porcentaje especificado.

Configuración del redireccionamiento de WAN

A continuación se describen los pasos a seguir para configurar el redireccionamiento de WAN. En el próximo apartado se da un ejemplo de cómo realizar dichas tareas.

Para configurar el redireccionamiento de WAN, necesita:

1. Configurar el enlace principal.
2. Configurar el enlace alternativo.
3. Asignar el enlace alternativo al enlace principal. También puede especificar un período de estabilización para el enlace principal.

   Puede especificar una hora de reversión al enlace principal, lo que se producirá después de que se termine el período de estabilización (si se ha configurado). Esto permite que el enlace secundario permanezca activo hasta la hora especificada por el usuario y que se revierta al enlace principal durante las horas en que el tráfico es menos intenso.

   Nota: Los tipos de enlace de datos de los enlaces principal y alternativo, pueden ser diferentes. Los enlaces principal y alternativo pueden ser de los tipos siguientes:
   - Una interfaz LAN.
   - Una interfaz PPP serie.
   - Una interfaz Frame Relay serie.
   - Una interfaz An X.25 serie.
   - Un circuito PPP de marcación.
   - Un circuito Frame Relay de marcación.

Ejemplo de configuración del redireccionamiento de WAN

La Figura 4 en la página 100 muestra el redireccionamiento de WAN utilizando un circuito Frame Relay de marcación sobre RDSI como enlace alternativo. Si el DLCI de Frame Relay entre los direccionadores A y C da un error, el redireccionamiento de WAN utilizará el circuito de marcación para establecer una conexión alternativa a través del direccionador D. Si uno de los enlaces principales

entre una de las sucursales y las oficinas centrales da un error, el redireccionamiento de WAN establece una ruta alternativa hasta las oficinas centrales a través de otra sucursal.

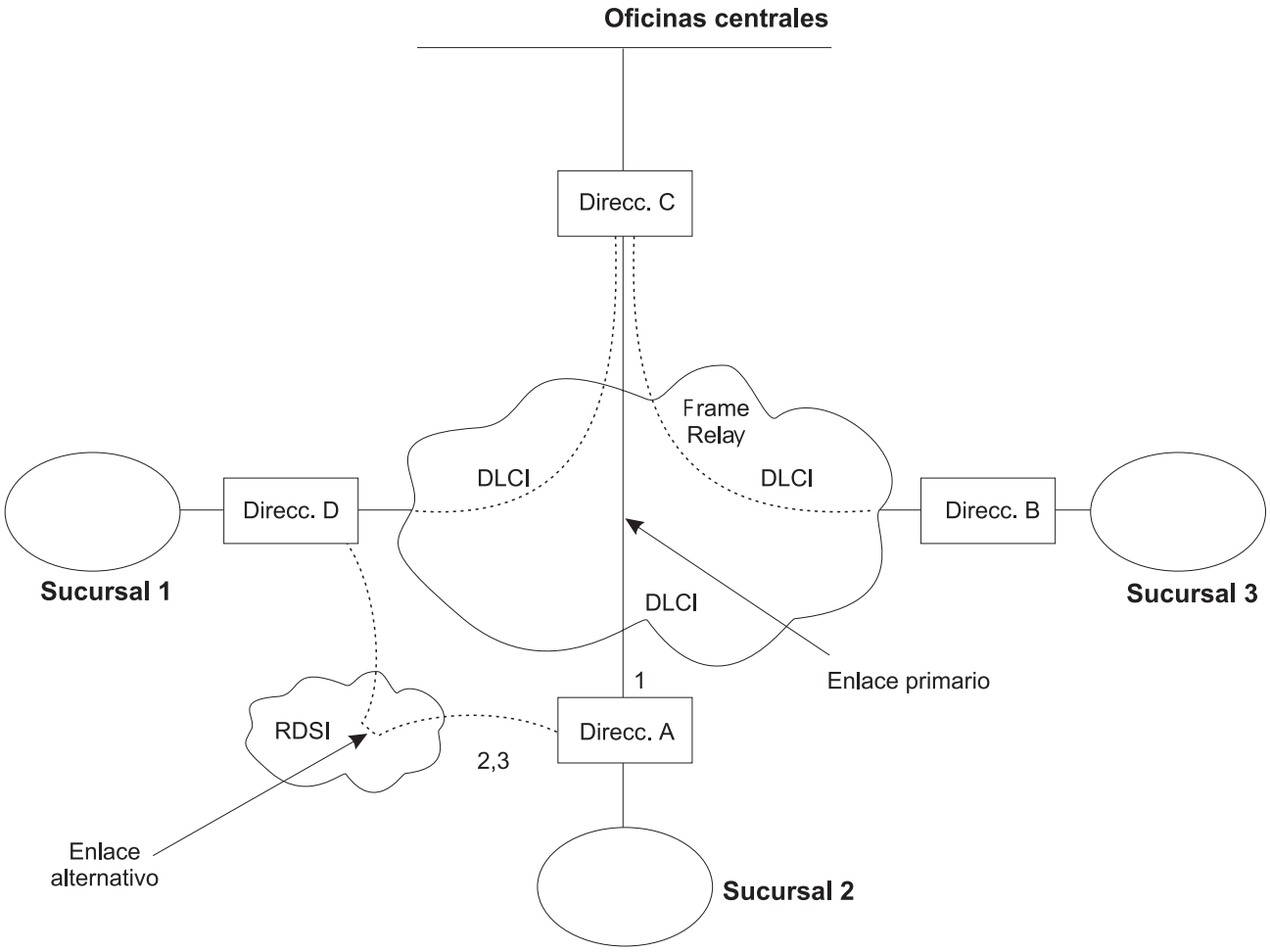


Figura 4. Ejemplo de configuración del redireccionamiento de WAN. Las sucursales utilizan Frame Relay para conectarse con las oficinas centrales.

En los apartados siguientes se describe cómo configurar el redireccionamiento de WAN en el direccionador A de la Figura 4. Se necesita:

- Configurar la interfaz Frame Relay principal (1) para que tenga un PVC obligatorio o un Grupo de PVC obligatorios, o habilitar la función Sin PVC para la interfaz Frame Relay.
- Configurar la interfaz RDSI (2) y su circuito de marcación Frame Relay (3).
- Asignar el circuito de marcación de forma que sea el enlace alternativo de la interfaz Frame Relay principal y ejecutar el mandato **set idle 0** en el indicador de marcación `Circuit Config>` para inhabilitar la marcación a petición para este circuito.
- Opcionalmente, se puede asignar:
  - Un período de tiempo de estabilización para el enlace principal,
  - Una ventana de tiempo de reversión para el enlace principal.

A continuación se describen con más detalle estas tareas.

Configuración de la interfaz Frame Relay

Para configurar la interfaz Frame Relay para el redireccionamiento de WAN, en el direccionador A, añada un PVC entre los direccionadores A y C de la interfaz Frame Relay principal.

Para hacer que la interfaz FR principal se declare desactivada cuando pierda la conexión con otro u otros direccionadores, tiene tres opciones:

1. Habilitar la función Sin PVC. Si se habilita esta función, la interfaz FR se desactiva cuando no hay PVC activos.
2. Configurar un PVC como obligatorio, pero sin incluirlo en un grupo de PVC obligatorios. En este caso, la interfaz FR se desactiva cuando el PVC queda inactivo.
3. Configurar un conjunto de PVC como obligatorios y que además formen un grupo de PVC obligatorios. En este caso, la interfaz FR se desactiva cuando todos los PVC de un grupo de PVC obligatorios quedan inactivos.

Para configurar la interfaz Frame Relay principal, siga los pasos siguientes:

1. Si todavía no lo ha hecho, establezca en enlace de datos de la interfaz RDSI como Frame Relay.

```
Config>set data-link frame relay
Interface Number [0]? 2
```

2. Entrar en el proceso de configuración de Frame Relay.

```
Config>network
What is the network number [0]?2
Frame Relay user configuration
FR Config>
```

   Nota: Para configurar la interfaz Frame Relay principal, sólo hay que llevar a cabo *uno* de los dos pasos siguiente.

3. Añadir un PVC con el mandato **add permanent-virtual-circuit**.

   Para configurar el PVC como Obligatorio:

   Escriba **y** (sí) a la pregunta “Is circuit required for interface operation ?” (¿El circuito es obligatorio para el funcionamiento de la interfaz?).

   Para configurar el PVC como un miembro de un grupo de PVC obligatorios:

   a. Responda **y** (sí) a la pregunta “Does circuit belong to a Required PVC group ?” (¿El circuito pertenece a un grupo de PVC obligatorios?).
   b. A la pregunta “What is the group name ?” (¿Cuál es el nombre del grupo?), responda escribiendo un nombre de grupo.

   Si ya ha añadido algún PVC, utilice el mandato **change permanent-virtual-circuit** para configurar el PVC como obligatorio y para asignarlo a un Grupo de PVC obligatorios, según corresponda. Para obtener más información, consulte el apartado Utilización de interfaces Frame Relay en el *Software de Access Integration Services Guía del usuario.*

```
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 []?grupo1
```

4. Si lo desea, habilite la función Sin PVC.

   Nota: Realice este paso *sólo* si se ha saltado el paso anterior.

   ```
   FR Config>enable no-pvc
   ```

Se pueden establecer parámetros adicionales para Frame Relay. Para obtener más información, consulte el apartado 'Utilización de Frame Relay' en el *Software de Access Integration Services Guía del usuario*.

Configuración de la interfaz RDSI y del circuito de marcación

Configure la interfaz RDSI y el circuito de marcación entre los direccionadores A y D. Para obtener más información sobre cómo configurar las interfaces RDSI y los circuitos de marcación, consulte el apartado 'Utilización de la interfaz RDSI' en el *Software de Access Integration Services Guía del usuario*.

A diferencia de lo que ocurre en el restablecimiento de WAN, deben configurarse protocolos direccionables en el circuito de marcación, que se utilizarán como enlace alternativo. Si los protocolos direccionables no puede dejar de enviar paquetes de mantenimiento, el enlace alternativo establecerá una conexión incluso si el redireccionamiento no es necesario. En este caso, si sólo quiere utilizar el enlace alternativo como redireccionador, inhabilite el circuito de marcación. Para inhabilitar el circuito de marcación, ejecute el mandato **disable interface** en el indicador `Config>`.

Si la interfaz RDSI tiene asignados varios circuitos de marcación, podrá establecer prioridades para uno de ellos. Si todos los canales B tienen circuitos de marcación activos en la interfaz física y un circuito con una prioridad mayor recibe un paquete, se concluirá la conexión que tenga la prioridad más baja y el circuito con mayor prioridad establecerá una conexión.

Las prioridades que se pueden definir están comprendidas entre 0 y 15, donde 15 es el circuito de mayor prioridad y 0 es el de menor prioridad. La prioridad por omisión para los circuitos de marcación nuevos es de 8. Escriba **set priority** en el indicador `Circuit Config>` para cambiar la prioridad.

Asignación y configuración del enlace alternativo

Entre en el proceso de configuración del redireccionamiento de WAN para asignar el circuito de marcación como enlace alternativo para una interfaz LAN, una interfaz PPP, Frame Relay, o X.25 serie, o un circuito de marcación PPP o Frame Relay y, si así lo desea, para especificar los períodos de estabilización y la ventana de tiempo de reversión.

Hay tres tipos de períodos de estabilización:

- *El primer período de estabilización* es el tiempo que el direccionador espera a que la interfaz principal se active la primera vez que el direccionador intenta activarla. Si, después del primer período de estabilización, la interfaz principal no se ha activado, el redireccionamiento WAN activa el enlace alternativo.

- *El período de estabilización* es el tiempo que el direccionador espera para asegurarse de que el enlace principal es fiable antes de revertir del enlace alternativo al enlace principal.
- *El período de estabilización de direccionamiento* es el tiempo que el direccionador mantiene ambos enlaces, el principal y el alternativo, después de revertir del enlace alternativo al enlace principal. Este tiempo sirve para que protocolos de direccionamiento como OSPF o RIP reconozcan la disponibilidad de la ruta nueva a través del enlace principal antes de que se desactive el enlace alternativo.

La ventana de tiempo de reversión es la hora del día concreta en que el usuario quiere revertir al enlace principal después de que esté activado y que haya transcurrido el tiempo de estabilización configurado.

El usuario especifica las horas de inicio y parada de la ventana de reversión utilizando un reloj en formato de 24 horas. El enlace secundario se mantiene activo y no se desactiva hasta que se alcanza la hora inicial. Si la hora del día en que se activa el enlace principal ocurre entre las horas inicial y final (dentro de la ventana), la reversión al enlace principal se produce inmediatamente después de que se termine el tiempo de estabilización.

Para asignar y configurar el enlace alternativo, siga estos pasos:

1. Entre en el proceso de configuración de redireccionamiento WAN.

```
Config>feature wrs
WAN Restoral user configuration
```

2. Asigne el circuito de marcación como enlace alternativo de la interfaz Frame Relay principal.

```
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 principal determinada, utilice el mandato **set first-stabilization-period**. Para definir un primer período de estabilización por omisión para todas las interfaces para las que no se ha especificado ningún período, 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 concretas, utilice el mandato **set stabilization-period**. Para definir un período de estabilización por omisión para todas las interfaces para las que no se ha especificado ningún período, 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]?
```

6. Opcionalmente, especifique un período de estabilización de rutas. Para definir un período de estabilización de rutas para interfaces concretas, utilice el mandato **set routing-stabilization**.

```
WRS Config>set routing-stabilization
Primary interface number [0]? 1
Routing stabilization time (0 - 3600 seconds) [15]?
```

7. Opcionalmente, especifique una ventana de tiempo de reversión.

   Para definir las horas inicial y final para ventanas de interfaces concretas, utilice los mandatos set start-time-of-day-revert-back y stop-time-of-day-revert-back. El valor por omisión es cero y significa que no hay ninguna ventana configurada. El reloj en formato de 24 horas empieza a la 1 a.m. y termina a medianoche, a las 24. Si las horas inicial y final son la misma (distintas de cero), el reversión se producirá exactamente a esa hora.

   A continuación se dan dos ejemplos de configuración de la ventana de reversión:

   a. Una hora inicial 23 y una hora final 3, dará una ventana de reversión de 11 p.m. a 3 a.m.
   b. Una hora inicial 1 y una hora final 5, dará una ventana de reversión de 1 a.m. a 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]?
```

Capítulo 8. Utilización de la característica Network Dispatcher

En este capítulo se describe cómo utilizar la característica Network Dispatcher y consta de los apartados siguientes:

- "Visión general de Network Dispatcher"
- "Reparto del tráfico TCP y UDP utilizando Network Dispatcher" en la página 106
- "Alta disponibilidad de Network Dispatcher" en la página 107
- "Configuración de Network Dispatcher" en la página 109
- "Utilización de Network Dispatcher con el servidor TN3270" en la página 116
- "Utilización de Network Dispatcher con Antememoria de servidor Web" en la página 117
- "Utilización de Network Dispatcher con eNetwork Host On-Demand Client Cache" en la página 118
- "Utilización de Network Dispatcher con la función SHAC (Scaleable High Availability Cache)" en la página 118

Network Dispatcher utiliza una tecnología de reparto de cargas desarrollada por la División de investigación de IBM, que determina qué servidor es el más adecuado para recibir una nueva conexión. Se trata de la misma tecnología que utiliza el producto eNetwork Dispatcher, de IBM, para Solaris, Windows NT y AIX.

Visión general de Network Dispatcher

La característica Network Dispatcher aumenta el rendimiento de los servidores al reenviar las peticiones de sesiones TCP/IP a distintos servidores pertenecientes a un grupo de servidores, repartiendo la carga de las peticiones entre todos los servidores. El reenvío es transparente para los usuarios y las aplicaciones. Network Dispatcher es útil en aplicaciones de servidor, como por ejemplo e-mail, servidores World Wide Web, consultas a bases de datos distribuidas en paralelo y otras aplicaciones TCP/IP.

Network Dispatcher también puede utilizarse para repartir la carga del tráfico de una aplicación UDP sin información de estado entre un grupo de servidores.

Network Dispatcher puede ayudarle a maximizar el potencial de su sede, proporcionándole una herramienta poderosa, flexible y escalable para solucionar los problemas de puntas de demanda. En períodos de puntas de demanda, Network Dispatcher puede encontrar automáticamente el servidor óptimo para manejar las peticiones entrantes.

La función Network Dispatcher no utiliza un servidor de nombres de dominio para repartir la carga. Distribuye el tráfico entre los servidores mediante una combinación exclusiva de software de reparto de carga y de gestión. Network Dispatcher también puede detectar un servidor que esté dando errores y reenviar el tráfico a otros servidores que estén disponibles.

Todas las peticiones de los clientes que se envían a la máquina Network Dispatcher se reenvían al servidor seleccionado por Network Dispatcher como servidor óptimo, según una serie de pesos establecidos dinámicamente. Puede utilizar los valores por omisión para dichos pesos o cambiar los valores en el proceso de configuración.

El servidor devuelve una respuesta al cliente sin la intervención de Network Dispatcher. Los servidores no necesitan ningún software adicional para comunicarse con Network Dispatcher.

La función Network Dispatcher es la clave para una gestión estable y eficiente de una red grande y escalable de servidores. Con Network Dispatcher puede enlazar varios servidores individuales en lo que aparenta ser un único servidor virtual. De esta forma, todo el mundo verá su sede como una sola dirección IP. Network Dispatcher funciona independientemente del servidor de nombres de dominio; todas las peticiones se envían a la dirección IP de la máquina Network Dispatcher.

Network Dispatcher permite que una aplicación de gestión basada en SNMP supervise el estado de Network Dispatcher al recibir estadísticas básicas y situaciones de alertas potenciales. En el apartado “Gestión de SNMP”, de la publicación *Configuración y supervisión de protocolos - Manual de consulta Volumen 1* hallará más información.

Network Dispatcher consigue ventajas evidentes en el reparto de la carga del tráfico entre un grupo de servidores, lo que redunda en una gestión estable y eficiente de su sede.

Reparto del tráfico TCP y UDP utilizando Network Dispatcher

El reparto de cargas se puede enfocar de muchas maneras. Algunos de esos enfoques permiten que los usuarios elijan un servidor distinto al azar en caso de que el primero vaya lento o no responda. Otro método es el de repartir la carga rotativamente, en el que el servidor de nombres de dominio elige un servidor para manejar las peticiones. Este enfoque es mejor, pero no tiene en cuenta la carga actual del servidor de destino, ni si está disponible.

Network Dispatcher puede repartir la carga de las peticiones de distintos servidores basándose en el tipo de petición, un análisis de la carga de los servidores o un conjunto configurable de pesos asignados por el usuario. Para gestionar cada tipo de reparto, Network Dispatcher dispone de los componentes siguientes:

Ejecutor Reparte la carga de las conexiones dependiendo del tipo de petición recibida. Los tipos de petición más corrientes son HTTP, FTP y Telnet. Este componente siempre está operativo.

Asesor Consulta a los servidores y analiza para cada uno los resultados obtenidos por cada protocolo. El asesor pasa esta información al ***gestor*** para establecer los pesos adecuados. El asesor es un componente opcional.

Network Dispatcher da soporte a asesores para FTP, HTTP, SMTP, NNTP, POP3 y Telnet, así como para TN3270, que funcionan con servidores TN3270 en los direccionadores IBM 2210, IBM 2212 e IBM 2216, y un asesor MVS que funciona con Workload Manager (WLM) en sistemas MVS. WLM gestiona la carga de trabajo de un sólo ID de MVS. Network Dispatcher puede utilizar WLM para ayudar a repartir la carga de las peticiones a los servidores MVS que ejecuten OS/390 V1R3 o posterior.

No existen asesores específicos para los protocolos UDP. Si tiene servidores MVS, puede utilizar el asesor del sistema MVS para proporcionar información de la carga del servidor. Además, si el puerto maneja tráfico TCP y UDP, puede utilizarse el asesor del protocolo TCP adecuado para proporcionar entrada al asesor para

el puerto. Network Dispatcher utilizará esta entrada para repartir la carga del tráfico TCP y UDP del puerto.

Gestor Establece pesos para un servidor basándose en los elementos siguientes:

- Contadores internos del ejecutor
- Realimentación de los servidores proporcionada por los asesores de los protocolos
- Realimentación de un supervisor del sistema (asesor MVS).

El gestor es un componente opcional. Sin embargo, si no utiliza el gestor, Network Dispatcher repartirá la carga según un método de planificación rotativo basado en los pesos actuales de los servidores.

Si utiliza Network Dispatcher para repartir la carga del tráfico UDP sin información de estado, deberá utilizar solamente servidores que respondan al cliente utilizando la dirección IP destino de la petición. Consulte “Configuración de un servidor para Network Dispatcher” en la página 114 para obtener una explicación más completa.

Alta disponibilidad de Network Dispatcher

La función base de Network Dispatcher tiene las características siguientes que, desde distintos puntos de vista, la convierten en el único punto en que se puede producir una anomalía:

- Examina todo el tráfico de entrada. Si algún paquete de una conexión existente utiliza una vía distinta a través de otro Network Dispatcher diferente para acceder a un servidor, éste, restablecerá inmediatamente la conexión.
- Hace un seguimiento de todas las conexiones establecidas y, aunque no las interrumpa, las entradas perdidas de la tabla de conexiones de Network Dispatcher provocarán el restablecimiento de una conexión.
- Aparece ante el direccionador de saltos anterior como el último salto y la finalización de la conexión.

Todas estas características hacen que las anomalías siguientes sean críticas para el cluster:

- Si Network Dispatcher da un error por alguna razón, se perderán todas las tablas de conexiones, por lo que también se perderán todas las conexiones existentes entre el cliente y el servidor. Suponiendo que exista un segundo Network Dispatcher capaz de dirigir un cliente a los servidores, podrán activarse nuevas conexiones después de los retardos del protocolo de direccionamiento habituales, que pueden ser de varios minutos.
- Si la interfaz de Network Dispatcher configurada para el direccionador de IP anterior da un error, debe poderse obtener otra interfaz para el mismo Network Dispatcher, en cuyo caso, el direccionador de IP realizará la recuperación (utilizando el mecanismo de ARP para determinar la antigüedad, con un retraso de varios minutos), o se perderán todas las conexiones.
- Si se produce una anomalía en la interfaz de Network Dispatcher con los servidores, el direccionador de saltos anterior, supone que Network Dispatcher es el último salto y, por lo tanto, no redireccionará las conexiones nuevas. Las conexiones existentes se perderán y no se establecerán conexiones nuevas.

En todos estos casos de error, que no son únicamente debidos a errores de Network Dispatcher, sino a errores producidos en sus proximidades, se perderán todas las conexiones existentes. Incluso con un Network Dispatcher de reserva que

ejecute los mecanismos estándar de recuperación de IP, la recuperación es, en el mejor de los casos, lenta y sólo es aplicable a las conexiones nuevas. En el peor de los casos, las conexiones no se podrán recuperar.

Para mejorar la disponibilidad de Network Dispatcher, la función Alta disponibilidad de Network Dispatcher utiliza los mecanismos siguientes:

- Dos Network Dispatcher conectados a los mismos clientes y al mismo grupo de servidores, así como entre ellos.
- Un mecanismo de "Latido" entre ambos Network Dispatcher capaz de detectar la anomalía de un Network Dispatcher.
- Un criterio de accesibilidad para identificar los sistemas principales IP que pueden o no pueden accederse desde cada Network Dispatcher.
- Sincronización de las bases de datos de Network Dispatcher (o sea, las tablas de conexiones, las tablas de accesibilidad y otras bases de datos).
- Lógica para elegir el Network Dispatcher activo, que está a cargo de un determinado grupo de servidores, y el Network Dispatcher en espera, que está continuamente sincronizado con ese grupo de servidores.
- Un mecanismo para tomar el control de IP rápidamente, cuando la lógica o un operador decide intercambiar el Network Dispatcher activo por el que está en espera.

Detección de anomalías

Además de los criterios básicos de detección de anomalías (pérdida de conexión entre los Network Dispatcher activo y en espera, detectada mediante los mensajes del mecanismo de Latido), hay otro mecanismo de detección de anomalías llamado "criterio de accesibilidad".Cuando se configura la función Network Dispatcher, se suministra una lista de sistemas principales a los que cada uno de los Network Dispatcher debe poder acceder para funcionar correctamente. Los sistemas principales pueden ser direccionadores, servidores IP u otros tipos de sistemas principales. La accesibilidad al sistema principal se determina sondeando el sistema principal.

El intercambio tiene lugar si no pueden aceptarse los mensajes del mecanismo de Latido, o si el Network Dispatcher activo ya no cumple el criterio de accesibilidad y el Network Dispatcher en espera es accesible. Para tomar una decisión en base a toda la información disponible, el Network Dispatcher activo envía regularmente al Network Dispatcher en espera sus posibilidades de accesibilidad. A continuación, el Network Dispatcher en espera compara dichas posibilidades de accesibilidad con las suyas y decide si debe realizarse el intercambio.

Sincronización de bases de datos

Los Network Dispatcher principal y de reserva mantienen sincronizadas sus bases de datos mediante el mecanismo de "Latido". La base de datos de Network Dispatcher contiene las tablas de conexiones, las tablas de accesibilidad y otra información. La función Alta disponibilidad de Network Dispatcher utiliza un protocolo de sincronización de bases de datos que garantiza que ambos Network Dispatcher contengan las mismas entradas de la tabla de conexiones. La sincronización tiene en cuenta un margen de error conocido debido a los retardos en la transmisión. El protocolo realiza una sincronización inicial de las bases de datos y a partir de entonces mantiene la sincronización de las bases de datos mediante actualizaciones periódicas.

Estrategia de recuperación

En caso de que se produzca una anomalía del Network Dispatcher, el mecanismo de toma de control de IP dirigirá rápidamente todo el tráfico hacia el Network Dispatcher en espera. El mecanismo de sincronización de bases de datos garantiza que el Network Dispatcher en espera tenga las mismas entradas que el activo. Si la anomalía se produce en la red (cualquier componente hardware o software que esté entre el cliente y el servidor final) y existe una vía alternativa a través del software en espera que funciona, el intercambio se realiza a través de la vía alternativa.

Toma de control de IP

Nota: Las direcciones IP del cluster se supone que están en la misma subred lógica que el direccionador de saltos anterior (direccionador IP).

El direccionador IP resolverá las direcciones del cluster mediante el protocolo ARP. Para realizar la toma de control de IP, el Network Dispatcher (en espera pero pasando a ser el activo) emitirá una petición ARP a sí mismo, que se difundirá a todas las redes directamente conectadas pertenecientes a la subred lógica del cluster. El direccionador IP de saltos anterior actualizará sus tablas ARP (según la RFC826) para enviar todo el tráfico de ese cluster al nuevo Network Dispatcher activo (antes en espera).

Configuración de Network Dispatcher

Hay varias formas de configurar Network Dispatcher para que dé soporte a su sede. Si la sede tiene sólo un nombre de sistema principal al que se conectarán todos los clientes, puede definir un único cluster y tantos puertos como quiera para recibir las conexiones. Esta configuración se muestra en la Figura 5.

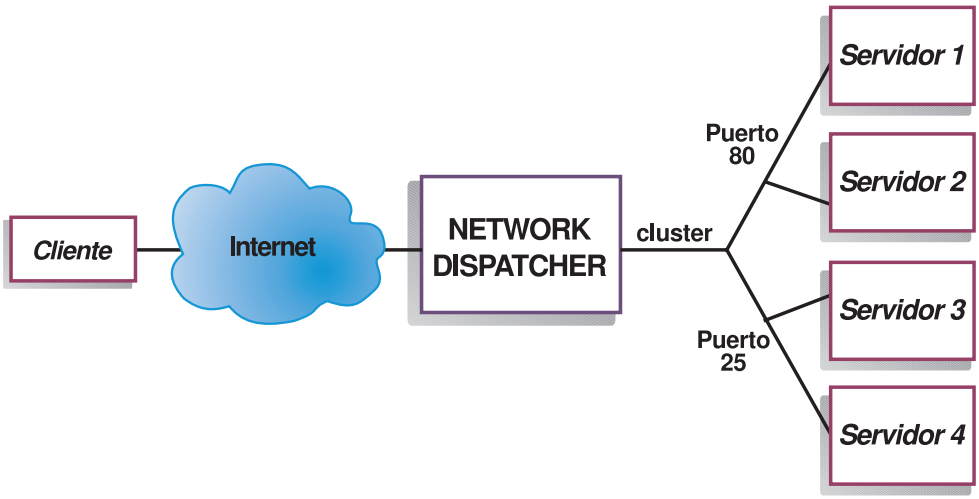


Figura 5. Ejemplo de Network Dispatcher configurado con un único cluster y 2 puertos

En caso de que la sede hospede el contenido de varias empresas o departamentos, que entren en la sede mediante URL distintos, sería necesario configurar Network Dispatcher de otra forma. En este caso, puede que le interese definir un cluster para cada empresa o departamento y para cada URL tantos puertos como quiera para recibir las conexiones, tal y como se muestra en la Figura 6 en la página 110.

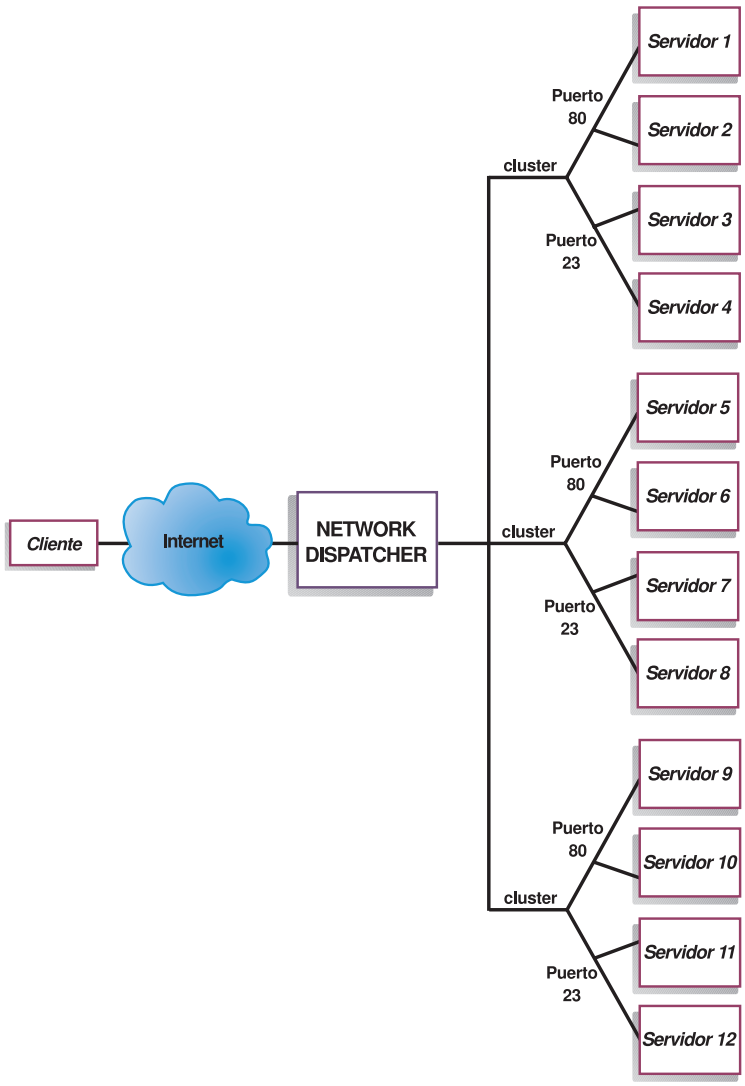


Figura 6. Ejemplo de Network Dispatcher configurado con 3 clusters y 3 URL

Una tercera forma de configurar Network Dispatcher sería apropiada si tuviera una sede muy grande con varios servidores dedicados a cada protocolo soportado. Por ejemplo, puede decidir tener servidores FTP independientes con líneas T3 directas para poder bajar archivos muy grandes. En este caso, puede que le interese definir un cluster para cada protocolo con un único puerto pero varios servidores, como se muestra en la Figura 7 en la página 111.

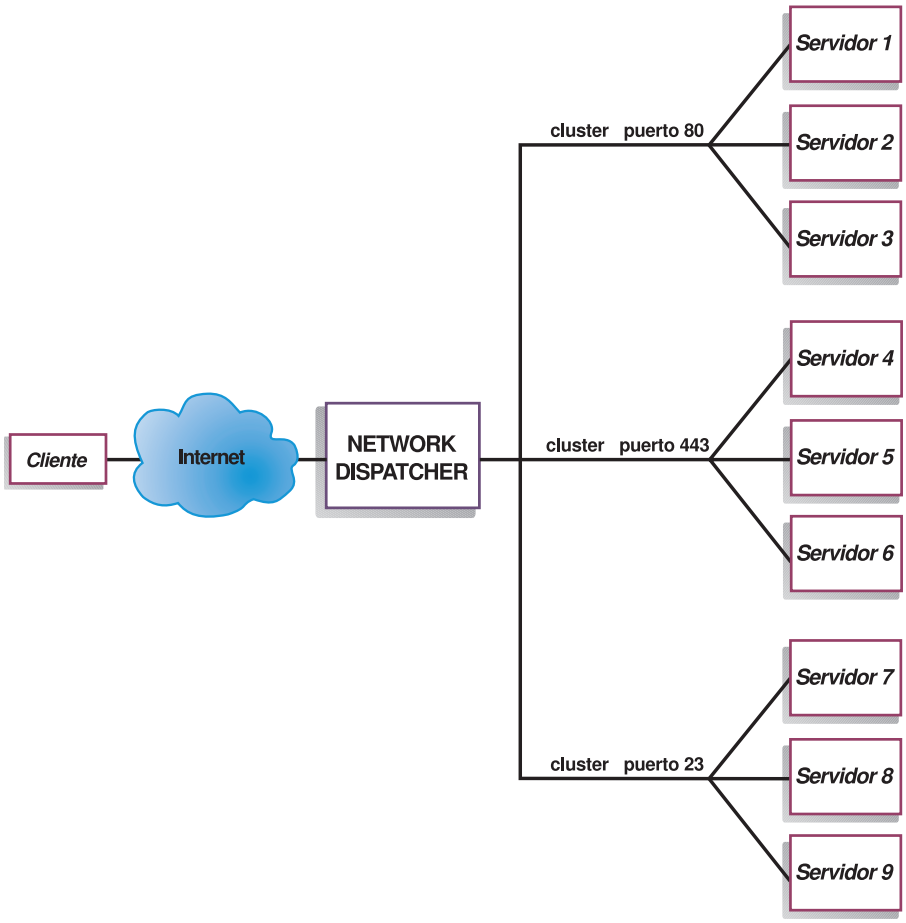


Figura 7. Ejemplo de Network Dispatcher configurado con 3 clusters y 3 puertos

Pasos para 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 forma que el tráfico saliente de los servidores a los clientes puede evitar pasar por el Network Dispatcher; sin embargo, usted no tendrá que configurar la conexión independiente.

   Si es importante que la red la disponibilidad de la red sea alta, en la Figura 8 en la página 112 se muestra una configuración de alta disponibilidad típica.

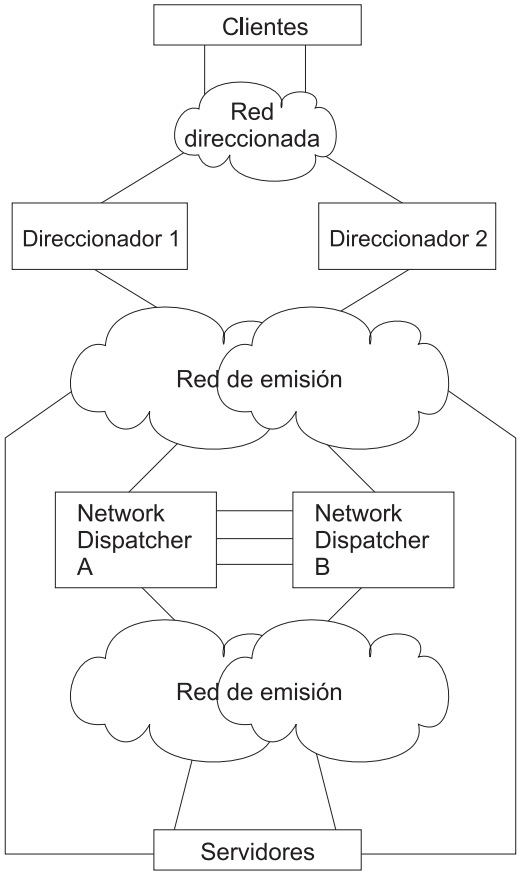


Figura 8. Configuración de Alta disponibilidad de Network Dispatcher

2. Configure las interfaces del dispositivo. Esto incluye configurar todas las interfaces, las direcciones IP de todas las interfaces y los protocolos de direccionamiento que se vayan a utilizar. Network Dispatcher utiliza la dirección IP interna del direccionador, de manera que también debe configurarse mediante el mandato set internal-ip-address. La dirección IP interna no debe coincidir con la dirección de un cluster configurado en Network Dispatcher.Consulte el capítulo Configuración y supervisión IP de la publicación *Configuración y supervisión de protocolos - Manual de consulta Volumen 1* para obtener más información sobre el mandato **set internal-ip-address**.
3. Vuelva a arrancar o iniciar el dispositivo.

Configuración de Network Dispatcher en un IBM 2212

Para configurar Network Dispatcher en un IBM 2212:

1. Acceda a la característica Network Dispatcher mediante el mandato **feature ndr**.
2. Habilite el ejecutor y el gestor mediante los mandatos **enable executor** y **enable manager**.
3. Configure los clusters utilizando el mandato add cluster. Network Dispatcher no anuncia específicamente las direcciones del cluster, lo que significa que deben seleccionarse las direcciones del cluster que forman parte de una subred anunciada local al direccionador de Network Dispatcher. Normalmente será la subred en la que Network Dispatcher reciba el tráfico de los clientes proveniente del direccionador de saltos siguiente.

Nota: La direcciones IP del cluster no deben coincidir con la dirección IP interna del direccionador ni con ninguna de las direcciones IP de interfaces definidas en el direccionador.

4. Configure los puertos TCP y UDP de destino mediante el mandato **add port** para cada cluster de servidores que sirvan al protocolo correspondiente. Ejemplo de puertos son: 80 para HTTP, 20 y 21 para FTP y 23 para Telnet.
5. Configure los servidores con el mandato **add server**.Un servidor siempre está asociado con un puerto y un cluster. Un servidor puede servir a más de un puerto, un puerto puede servir a más de un servidor y un servidor puede pertenece a más de un cluster, si el sistema operativo del servidor da soporte al uso de seudónimos.
6. Configure los asesores utilizando el mandato **add advisor**.

   Notas:

   a. Para el asesor MVS, no defina el valor Número de puerto (por omisión = 10007) para ningún cluster. El asesor MVS utiliza este número de puerto únicamente para comunicarse con WLM en los sistemas MVS.

   b. Para el asesor TN3270, se entran dos valores de puerto. El valor Número de puerto utilizado para la comunicación cliente-servidor (por omisión = 23) debe definirse para los clusters adecuados. No defina el valor Puerto de comunicaciones (por omisión = 10008) para ningún cluster. El asesor TN3270 utiliza el valor Puerto de comunicaciones solamente para reunir información sobre la carga de los servidores TN3270.
7. Habilite mediante el mandato **enable advisor** los asesores configurados.

si va a configurar Network Dispatcher para alta disponibilidad, siga los pasos siguientes. De lo contrario, ya se ha terminado la configuración.

Nota: Realice estos pasos primero en el Network Dispatcher principal y después en el de reserva. Para garantizar que la sincronización de las bases de datos sea la adecuada, debe habilitarse el ejecutor en el Network Dispatcher principal antes que en el de reserva.

8. Con el mandato **add backup**, configure si el Network Dispatcher es el principal o el de reserva y si el intercambio es manual o automático.
9. Configure todas las vías en las que se situará el mecanismo de latido entre los Network Dispatcher principal y de reserva, utilizando el mandato **add heartbeat**. Una vía se especifica definiendo las direcciones IP origen y destino. Es muy recomendable configurar más de una vía para el latido entre los Network Dispatcher, lo que garantizará que en caso de error de una sola interfaz, no se interrumpa la comunicación de latidos entre las máquinas principal y de reserva.
10. Con el mandato **add reach**, configure la lista de direcciones IP de sistemas principales a las que debe poder acceder Network Dispatcher para garantizar un servicio completo. Generalmente, consistirá en un subconjunto de servidores, el direccionador de la empresa o una estación de administración.

La configuración se puede cambiar mediante los mandatos **set**, **remove** y **disable**. Consulte el Capítulo 9, “Configuración y supervisión de la característica Network Dispatcher” en la página 121 para obtener más información sobre dichos mandatos.

Configuración de un servidor para Network Dispatcher

Para configurar un servidor para utilizarlo con Network Dispatcher:

1. Cambie el nombre al dispositivo bucle de retorno.

   Para que los servidores TCP y UDP funcionen, debe establecer (o mejor cambiarle el nombre) el dispositivo bucle de retorno (normalmente denominado ***lo0***) a la dirección del cluster. Network Dispatcher no modifica la dirección IP destino del paquete IP antes de reenviarlo a un servidor. Al establecer o cambiar el nombre del dispositivo bucle de retorno a la dirección del cluster, el servidor aceptará paquetes dirigidos a la dirección del cluster.

   Es importante que el servidor utilice la dirección del cluster en lugar de su propia dirección IP para responder al cliente.Esto no tiene importancia con los servidores TCP, pero algunos servidores UDP utilizan sus propias direcciones IP cuando responden a las peticiones enviadas a la dirección del cluster. Cuando el servidor utiliza sus propias direcciones IP, algunos clientes descartarán la respuesta del servidor ya que no proviene de una dirección IP origen esperada. Debe utilizar solamente servidores UDP que utilicen la dirección IP destino de la petición cuando respondan al cliente. En este caso, la dirección IP destino de la petición es la dirección del cluster.

   Si el sistema operativo da soporte al uso de seudónimos para la interfaz de red, como es el caso de AIX, Solaris o Windows NT, deberá cambiar el nombre del dispositivo bucle de retorno a la dirección del cluster. La ventaja de utilizar un sistema operativo que use seudónimos es que podrá configurar los servidores para que sirvan a varias direcciones de cluster.

   Si el sistema operativo del servidor no da soporte al uso de seudónimos, como es el caso de HP-UX y OS/2, deberá definir ***lo0*** como dirección del cluster.

   Si el servidor es un sistema MVS ejecutando TCP/IP V3R2, deberá definir la dirección VIPA como dirección del cluster. Esto funcionará como dirección del bucle de retorno. La dirección VIPA no debe pertenecer a una subred que esté directamente conectada con el nodo MVS. Si el sistema MVS ejecuta TCP/IP V3R3, deberá definir el dispositivo bucle de retorno como la dirección del cluster. Si utiliza la función de alta disponibilidad, deberá habilitar RouteD en el sistema MVS para que el mecanismo de intercambio de la función de alta disponibilidad funcione correctamente.

   Nota: La lista de mandatos que aparecen en este capítulo se han probado en las versiones de los sistemas operativos siguientes: AIX 4.1.5 y 4.2, HP-UX 10.2.0, Linux, OS/2 Warp Connect Version 3.0, OS/2 Warp Version 4.0, Solaris 2.5 (Sun OS 5.5) y Windows NT 3.51 y 4.0.

   Utilice el mandato que corresponda a su sistema operativo, tal y como se muestra en la Tabla 10 para definir el dispositivo bucle de retorno o cambiarle el nombre.

Tabla 10 (Página 1 de 2). Mandatos para cambiar el nombre del dispositivo bucle de retorno (lo0) para Dispatcher

Sistema	Mandato
AIX	**ifconfig lo0 alias** *dirección_cluster*
HP-UX	**ifconfig lo0** *dirección_cluster*
Linux	**ifconfig lo:1 dirección_cluster netmask up**
OS/2	**ifconfig lo dirección_cluster**

Tabla 10 (Página 2 de 2). Mandatos para cambiar el nombre del dispositivo bucle de retorno (lo0) para Dispatcher

Sistema	Mandato
Solaris	**ifconfig lo0:1 dirección_cluster 127.0.0.1 up**
Windows NT	1. Pulse en Inicio y después en Configuración. 2. Pulse en Panel de control y pulse dos veces en Red. 3. Si todavía no lo ha hecho, añada el Controlador del adaptador de bucle de retorno de MS. a. En la ventana Red, pulse en Adaptadores. b. Elija el Adaptador de bucle de retorno de MS y pulse en Aceptar. c. Cuando se le solicite, inserte el CD o los discos de instalación. d. En la ventana Red, pulse en Protocolos. e. Elija el Protocolo TCP/IP y luego pulse en Propiedades. f. Elija el Adaptador de bucle de retorno de MS y pulse en Aceptar. 4. Establezca la dirección del bucle de retorno a la dirección del cluster. Acepte la máscara de subred por omisión (255.0.0.0) y no escriba ninguna dirección para la pasarela (gateway). **Nota:** Es posible que tenga que salir y volver a entrar en la Configuración de red antes de que aparezca el Controlador de bucle de retorno de MS en la Configuración TCP/IP.

2. Compruebe la existencia de rutas de más.

   En algunos sistemas operativos puede ser que se cree un ruta por omisión que debe eliminarse.

   a. Compruebe la existencia de rutas de más en Windows NT utilizando el mandato siguiente: **route print**

   b. Compruebe la existencia de rutas de más en los sistemas UNIX y en OS/2 con el mandato siguiente: **netstat -nr**

   c. Ejemplo de Windows NT: Después de escribir el mandato route print, se mostrará una tabla parecida a esta: (En este ejemplo se muestra cómo buscar y eliminar una ruta de más para el cluster 9.67.133.158 con una máscara de red por omisión 255.0.0.0.)

```
Rutas activas:
Dirección de red          Máscara         Gateway         Interfaz    Métrica
              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 la dirección del cluster bajo la columna "Gateway". Si hay una ruta de más, la dirección del cluster aparecerá dos veces. En el ejemplo anterior, la dirección del cluster (9.67.133.158) aparece en la fila 2 y en la fila 8.

   e. Busque la dirección de red correspondiente a las filas en las que aparece la dirección del cluster. Una de las rutas es necesaria y la otra debe eliminarse, ya que es ajena. La ruta de más que debe ser eliminada será aquella cuya dirección de red empiece con el primer dígito de la dirección

del cluster, seguida de tres ceros. En el ejemplo anterior, la ruta de más es la de la fila dos, cuya dirección de red es 9.0.0.0:

```
9.0.0.0         255.0.0.0      9.67.133.158      9.67.133.158      1
```

3. Elimine todas las rutas de más.

   En la Tabla 11 se muestran los mandatos de cada sistema operativo que sirven para eliminar las rutas de más.

Tabla 11. Mandatos para eliminar rutas en varios sistemas operativos

Sistema operativo	**Mandato**
AIX	**route delete -net** *dirección_red dirección_cluster*
HP-Unix	**route delete** *dirección_cluster dirección_cluster*
Solaris	No es necesario eliminar rutas.
OS/2	No es necesario eliminar rutas.
Windows NT	**route delete** *dirección_red dirección_cluster* **Nota:** Este mandato debe entrarse en el indicador de mandatos de MS-DOS.

Utilización de Network Dispatcher con el servidor TN3270

Network Dispatcher puede utilizarse con clusters de direccionadores 2210, 2212, Utilidades de red o 2216 ejecutando la función de servidor TN3270 para dar soporte de servidor TN3270E en entornos 3270 grandes. El asesor TN3270 permite que Network Dispatcher recoja estadísticas de la carga de cada servidor TN3270E en tiempo real con el fin de lograr 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 (puede ejecutarse en el mismo direccionador que Network Dispatcher).

Puntos clave para la configuración

La configuración de los servidores TN3270E esencialmente es la misma, exista o no Network Dispatcher para los servidores. De hecho, al servidor TN3270E no le importa si el tráfico proveniente de los clientes se despacha en otra máquina. Sin embargo, hay que tener en cuenta determinadas cuestiones al configurar los servidores TN3270 externos si se utilizan con Network Dispatcher:

- Puesto que Network Dispatcher no modifica la dirección IP destino de los paquetes (la dirección del cluster), que reenvía a los servidores, la dirección IP del servidor TN3270 de cada servidor debe ser igual que la dirección IP del cluster.
- Los direccionadores que ejecuten la función servidor TN3270 deben conocer la dirección IP de la función TN3270 que se ejecuta en el direccionador, para poder entregar paquetes a la función servidor. Por lo tanto, la dirección IP del servidor TN3270 (la dirección del cluster) también debe definirse para cada direccionador de servidor TN3270 así como la dirección IP interna del direccionador, o como dirección secundaria de 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 anuncien la dirección del cluster. El direccionador de Network Dispatcher debe “poseer” la dirección del

cluster, en lo que concierne a la red del cliente. Network Dispatcher no anuncia específicamente las direcciones del cluster, pero las direcciones del cluster deben seleccionarse para que formen parte de una subred anunciada local al direccionador de Network Dispatcher.

- Si el tráfico que va del cliente a Network Dispatcher se transmite por la misma LAN que el tráfico que va del Network Dispatcher al servidor, deberá asegurarse de que los servidores no respondan al ARP para la dirección del cluster, así que la dirección del cluster no puede definirse en la interfaz del servidor de esta LAN. Network Dispatcher debe ser el único que responda al ARP en la LAN en la que se recibe el tráfico de los clientes. La dirección del cluster puede configurarse alternativamente en el servidor TN3270 como una dirección de interfaz de otra interfaz, o puede configurarse como la dirección IP interna del servidor TN3270.
- Cada servidor TN3270 debe configurarse en Network Dispatcher con una dirección IP de servidor exclusiva. Esta dirección también debe configurarse como una dirección de interfaz en el direccionador que haga funciones de servidor TN3270.

Cuando el servidor TN3270 está en el mismo direccionador que Network Dispatcher, se aplica lo siguiente:

- La dirección IP del servidor TN3270 para el servidor TN3270 interno debe establecerse como la dirección del cluster, pero para el servidor interno, esta dirección no debe definirse en el direccionador como dirección IP interna ni como dirección de interfaz.
- Si el servidor TN3270 es externo, la dirección IP del servidor TN3270 debe definirse en el direccionador como la dirección IP interna o como una dirección de interfaz. Si el servidor TN3270 es interna, la dirección IP del 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 como ambos, y no puede conmutar entre ambas configuraciones. Debido a ello, al implementar una solución de alta disponibilidad de Network Dispatcher con servidores TN3270 internos en ambos direccionadores de Network Dispatcher, el Network Dispatcher de uno de los direccionadores, no podrá repartir la carga del servidor TN3270 del otro direccionador.Podrá repartir la carga de su propio servidor interno así como de los servidores configurados como externos.

LU explicitas y Network Dispatcher

Se ha de ser muy cuidadoso con la definición explícita de LU en un entorno de Network Dispatcher. Una petición de sesión en una LU implícita o explícita puede ser despachada a cualquier servidor. Esto significa que la LU explícita tiene que definirse en todos los servidores, puesto que no se sabe con antelación a que servidor se despachará la sesión.

Utilización de Network Dispatcher con Antememoria de servidor Web

Deberá utilizar Network Dispatcher para definir un cluster y un puerto para la Antememoria del servidor Web. Al definir un puerto con modalidad *antememoria*, se le pedirá que configure la partición de antememoria. Para ver un ejemplo, consulte el mandato **add port** en Capítulo 12, “Configuración y supervisión de la Antememoria de servidor Web” en la página 201. Los valores de configuración de una partición de antememoria pueden modificarse más adelante mediante el mandato **f webc** en el indicador `Config>`, que le permitirá ir directamente a la

configuración de la función Antememoria de servidor Web. Consulte el Capítulo 11, “Utilización de la Antememoria de servidor Web” en la página 165 y Capítulo 12, “Configuración y supervisión de la Antememoria de servidor Web” en la página 201 para obtener más información sobre Antememoria de servidor Web.

Utilización de Network Dispatcher con eNetwork Host On-Demand Client Cache

Deberá utilizar Network Dispatcher para definir un cluster y un puerto para Host On-Demand Client Cache. Al definir un puerto con modalidad *hod client cache*, se le pedirá que configure la partición de antememoria. Se muestra un ejemplo del mandato **add port** en “Configuración de Host On-Demand Client Cache” en la página 151. Los valores de configuración de una partición de antememoria pueden modificarse más adelante ejecutando el mandato **f hod** en el indicador `Config>`, que le permitirá ir directamente a la configuración de la característica Host On-Demand Client Cache. Para obtener más información sobre la función Host On-Demand Client Cache, consulte el Capítulo 10, “Configuración y supervisión de Host On-Demand Client Cache para eNetwork de IBM” en la página 151.

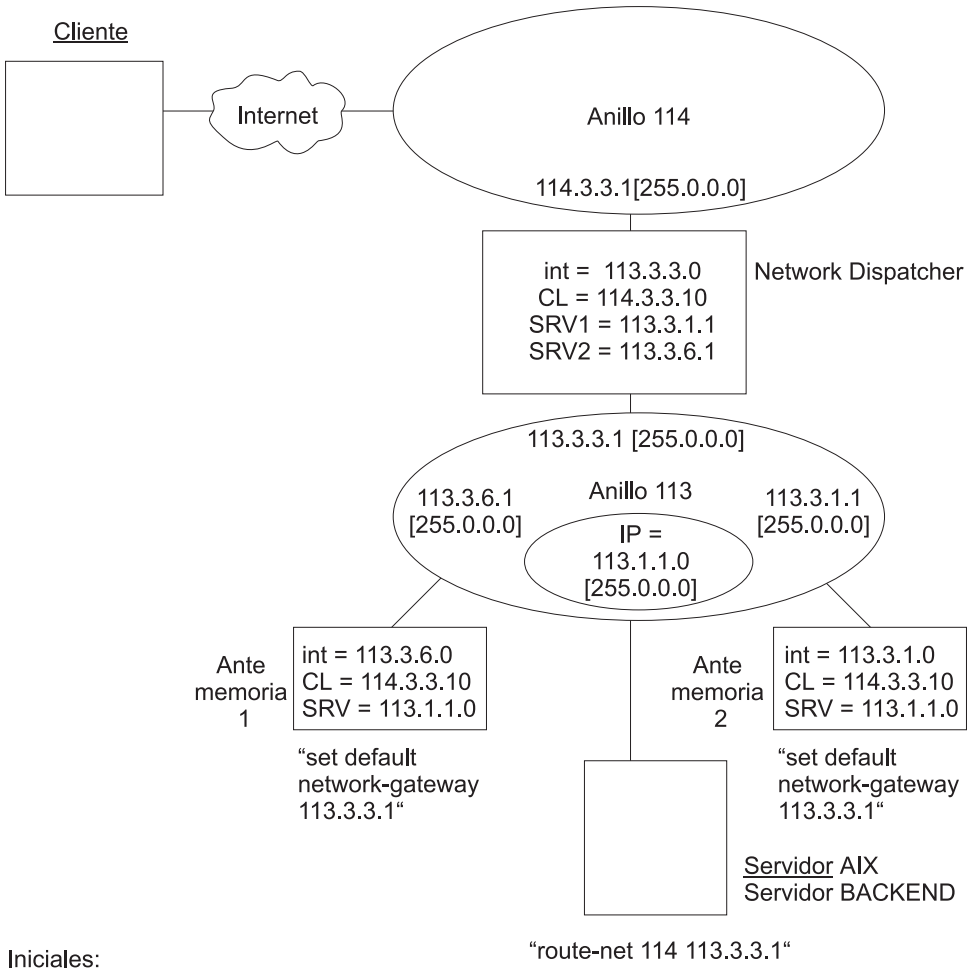
Utilización de Network Dispatcher con la función SHAC (Scaleable High Availability Cache)

En este apartado se describe cómo utilizar Network Dispatcher con la función Scaleable High Availability Cache (SHAC) y la Figura 9 en la página 119 muestra un diagrama de una SHAC en una red. La SHAC consiste en un grupo de antememorias de servidores Web más un Network Dispatcher independiente; las antememorias se configuran como servidores en Network Dispatcher. Las antememorias de un grupo comparten un cluster y puerto común. Los valores idénticos de cluster y puerto se programan en Network Dispatcher. La modalidad del puerto se define como `extcache` para indicar que suministra datos a un conjunto de antememorias escalables externas. Consulte el mandato **add port** en “Add” en la página 121.

Nota: En el Network Dispatcher puede ubicarse más de un grupo de antememorias.

El asesor y el gestor son críticos para la SHAC. El asesor HTTP debe habilitarse en todos los puertos para el que existan SHAC. Las consultas del asesor sirven para determinar si las antememorias configuradas están funcionando. Inicialmente, al establecer la conexión, las conexiones se dirigen a las antememorias basadas en el gestor. Por lo tanto, las proporciones del gestor deben establecerse de forma que incorporen al asesor. Esto es importante si las antememorias pasan a estar habilitadas o inhabilitadas.

Como otros servidores, las direcciones IP de interfaz de las antememorias se utilizan como direcciones del servidor. En la Figura 9 en la página 119 se muestra un ejemplo. Incluye las direcciones IP, máscaras de red e información de direccionamiento más importante. En la práctica, la mayoría de clientes se encontrarán en Internet. En cualquier caso, la ruta del cliente a las antememorias debe pasar por el Network Dispatcher (razón por la que los clientes no pueden estar conectados al anillo 113 del dibujo).



Iniciales:

CL: Dirección de cluster. Nota - en este ejemplo se asume el uso del puerto 80, el puerto http por omisión.
INT: Dirección interna para el direccionador 22XX
SRV: Dirección(es) de servidor asociadas con CL
"....": mandatos de direccionamiento adicionales para establecer la conectividad.

Figura 9. Dos antememorias con Network Dispatcher, un cliente y un servidor final.

Capítulo 9. Configuración y supervisión de la característica Network Dispatcher

En este capítulo se describen los mandatos de configuración y de funcionamiento de la característica Network Dispatcher. Consta de los apartados siguientes:

- "Acceso a los mandatos de configuración de Network Dispatcher"
- "Mandatos de configuración de Network Dispatcher"
- "Acceso a los mandatos de supervisión del Network Dispatcher" en la página 140
- "Mandatos de supervisión del Network Dispatcher" en la página 141

Acceso a los mandatos de configuración de Network Dispatcher

Para acceder al entorno de configuración de Network Dispatcher:

1. Escriba **talk 6** en el indicador OPCON (*).
2. Escriba **feature ndr** en el indicador `Config >`.

Mandatos de configuración de Network Dispatcher

En la Tabla 12 se resumen los mandatos de configuración de Network Dispatcher y el resto del apartado se dedica a explicar los mandatos. Entre los mandatos en el indicador `NDR Config >`.

Tabla 12. Mandatos de configuración de Network Dispatcher

Mandato	Función
? (Ayuda)	Visualiza todos los mandatos disponibles para este nivel de mandato, o lista las opciones de mandatos específicos (si es que están disponibles). Consulte "Obtención de ayuda" en la página xxv.
Add	Configura varios componentes del Network Dispatcher, incluyendo asesores, clusters, puertos y servidores.
Clear	Borra toda la configuración del Network Dispatcher.
Disable	Inhabilita los componentes ejecutor, gestor y de reserva del Network Dispatcher. También inhabilita asesores concretos.
Enable	Habilita los componentes ejecutor, gestor y de reserva del Network Dispatcher. También habilita asesores concretos.
List	Muestra toda la configuración del Network Dispatcher, o partes concretas de la configuración.
Remove	Elimina partes concretas de la configuración del Network Dispatcher.
Set	Cambia los parámetros de configuración de asesores, clusters, puertos, servidores o el gestor del Network Dispatcher.
Exit	Hace volver al nivel de mandato anterior. Consulte "Salida de un entorno de nivel inferior" en la página xxv.

Add

Utilice el mandato **add** para configurar asesores, clusters, puertos, servidores y direcciones accesibles. Para la función Alta disponibilidad también puede configurar si este Network Dispatcher es el principal o el de reserva y qué

direcciones IP utilizar para el mecanismo de latido y para la sincronización de bases de datos.

Sintaxis:

add advisor . . .
backup . . .
cluster . . .
heartbeat . . .
port . . .
reach . . .
server . . .

Advisor *nombre núm-puerto intervalo tiempo-espera puerto-com*

Especifica el nombre y el puerto de un asesor. Este parámetro también especifica con qué frecuencia reunirá información el asesor para un protocolo determinado y un período de tiempo después del cual el asesor considerará que el protocolo no está disponible.

nombre

Especifica el tipo de asesor.

Tabla 13. Nombres y números de puerto del asesor

Número de asesor	Nombre de asesor	Número de 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: de 0 a 7

Valor por omisión: 1

núm-puerto

Especifica el número de puerto del asesor.

Valores válidos: de 1 a 65535

Valores por omisión: Consulte la Tabla 13.

intervalo

Especifica la frecuencia, en segundos, con que el asesor consulta a su protocolo para cada servidor. Transcurrida la mitad del intervalo sin obtener respuesta por parte del servidor, el asesor considera que el protocolo no está disponible.

Valores válidos: de 0 a 65535

Valor por omisión: 5

tiempo de espera

Especifica el intervalo de tiempo, en segundos, después del cual el asesor considera que el protocolo no está disponible.

Para asegurarse de que el gestor no utiliza información desfasada en las decisiones que debe tomar sobre el reparto de la carga, el gestor no utilizará la información suministrada por el asesor cuya indicación de la hora sea anterior a la hora definida en este parámetro. El tiempo de espera del asesor debe ser mayor que el intervalo de sondeo del asesor. Si el tiempo de espera es menor, el gestor no hará caso de los informes que debe utilizar. Por omisión, los informes del asesor no tienen tiempo de espera.

Lo normal es que se utilice este valor si se inhabilita un asesor. No confunda este parámetro con el tiempo de espera de la mitad del intervalo descrito antes, que tiene que ver con la falta de respuesta de un servidor.

Valores válidos: de 0 a 65535

Valor por omisión: 0, lo que significa que se considera que el protocolo siempre está disponible.

puerto-com

Especifica el número de puerto utilizado por el asesor TN3270 para comunicarse con los servidores TN3270. Este parámetro es sólo de entrada para el asesor TN3270.

Valores válidos: de 1 a 65535

Valor por omisión: 10008

Nota: Como el componente gestor es requisito previo para el funcionamiento del asesor, debe habilitarse el gestor antes de poder habilitar los asesores. Al configurar los pesos del servidor, utilizados para tomar decisiones sobre el reparto de la carga, también deberá definir las proporciones del gestor para que el gestor tenga en cuenta las entradas de los asesores. También debe definir la dirección ip interna con el mandato **set internal-ip-address** para que el asesor funcione correctamente. Consulte Configuración y supervisión IP, en *Configuración y supervisión de protocolos - Manual de consulta Volumen 1* para obtener más información sobre el mandato **set internal-ip-address**.

Ejemplo 1:

```
add advisor
Advisor name (0=ftp,1=http,2=MVS,3=TN3270,4=smtp,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=smtp,5=nntp,6=pop3,7=telnet) [1]? 3
Port number [23]?
Interval (seconds) [5]? 10
Timeout (0=unlimited) [0]? 10
Communication Port number [10008]?
```

backup *cometido estrategia*

Especifica si este Network Dispatcher es el principal o el de reserva.

cometido

Define si este es el Network Dispatcher principal o el de reserva. Utilice este mandato sólo si quiere tener una configuración redundante y si quiere ejecutar la función de Alta disponibilidad.

En este caso, también deberá configurar el mecanismo de latido (**add heartbeat**) y de accesibilidad (**add reach**).

Valores válidos: 0 ó 1

0 = principal

1 = de reserva

Valor por omisión: 0

estrategia

Especifica si el Network Dispatcher volverá a la modalidad principal automática o manualmente. Si se produce una anomalía en el Network Dispatcher principal y pasa a modalidad de espera (lo que quiere decir que la función de toma de control de IP realizará una copia de seguridad) y a continuación vuelve a estar disponible, se convertirá automáticamente en el Network Dispatcher activo, si la estrategia se define como *automática*, tan pronto como las bases de datos se sincronicen. Si la estrategia se define como *manual*, el primer Network Dispatcher principal pasará a modalidad de espera y el operador deberá utilizar el mandato **switchover** en talk 5 para volver a activarlo. Consulte “Switchover” en la página 148.

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 *dirección cuenta-FIN tiempo-espera-FIN temporizador-inactividad*

Especifica la dirección IP de un cluster y la frecuencia con que el ejecutor realizará la recogida de basura de la base de datos del Network Dispatcher. Network Dispatcher no anuncia específicamente las direcciones del cluster, lo que significa que deben seleccionarse las direcciones del cluster que forman parte de una subred anunciada que es local al direccionador del Network Dispatcher. Normalmente será la subred en la que el Network Dispatcher recibe el tráfico de los clientes proveniente del siguiente direccionador de salto.

Nota: La direcciones IP del cluster no deben coincidir con la dirección IP interna del direccionador ni con ninguna de las direcciones IP de interfaces definidas en el direccionador.

dirección

Especifica la dirección IP del cluster.

Valores válidos: Cualquier dirección IP

Valor por omisión: 0.0.0.0

cuenta de FIN

Especifica el número de conexiones que deben estar en el estado FIN antes de que el ejecutor intente eliminar la información de conexión no usada de la base de datos del Network Dispatcher

después de transcurrido el *tiempo de espera de FIN* o el definido en el *temporizador de inactividad*.

Valores válidos: de 0 a 65535

Valor por omisión: 4000

tiempo de espera de FIN
Especifica el número de segundos que una tarea puede permanecer en el estado de FIN antes de que el ejecutor intente eliminar la información de conexión no usada de la base de datos del Network Dispatcher.

Valores válidos: de 0 a 65535

Valor por omisión: 30

Temporizador de inactividad
Especifica el número de segundos que el ejecutor esperará que una conexión esté inactiva, antes de intentar eliminar la información de la conexión de la base de datos del 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 *dirección1 dirección2*
Especifica una vía para los mensajes del mecanismo de Latido. Se recomienda que configure más de una entrada para que el comportamiento sea fiable. El mensaje del mecanismo de Latido se trasmitirá de la *dirección1*, perteneciente a este Network Dispatcher, a la *dirección2*, que pertenece al igual del Network Dispatcher.

dirección1
Especifica la dirección IP de la interfaz de este Network Dispatcher desde la que se transmiten los mensajes del mecanismo de Latido.

Valores válidos: Cualquier dirección IP.

Valor por omisión: 0.0.0.0

dirección2
Especifica la dirección IP de la interfaz del igual del Network Dispatcher que recibe los mensajes del mecanismo de Latido. Esta dirección debe ser accesible desde la interfaz especificada en la *dirección1*.

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 *dirección-cluster núm-puerto tipo-puerto peso-máx modalidad-puerto*

Especifica el puerto y sus atributos.

dirección-cluster

Especifica la dirección IP del cluster.

Valores válidos: Cualquier dirección IP.

Valor por omisión: 0.0.0.0

núm-puerto

Especifica el número de puerto del protocolo para este cluster.

Valores válidos: de 1 a 65535

Valor por omisión: 80

tipo-puerto

Especifica los tipos de tráfico IP cuya carga puede repartirse en este puerto. Los tipos soportados son:

- 1 = TCP
- 2 = UDP
- 3 = ambos

Valores válidos: 1, 2, 3

Valor por omisión: 3

peso-máx

Especifica el peso máximo para los servidores de este puerto. Esto afecta a la diferencia que habrá en el número de peticiones que el ejecutor entregará a cada servidor.

Valores válidos: de 0 a 100

Valor por omisión: 20

modalidad-puerto

Especifica si el puerto enviará todas las peticiones de un único cliente a un único servidor (llamado adherente), utilizará ftp pasivo (pftp), utilizará la Antememoria de servidor Web (antememoria), las enviará a un conjunto de antememorias escalables externas (antememoria externa), utilizará Host On-Demand Client Cache, o no utilizará ningún protocolo particular para este cluster (ninguno).

Valores válidos: 0 - 5, donde:

- 0 = none (ninguna)
- 1 = sticky (adherente)
- 2 = pftp
- 3 = cache (antememoria)
- 4 = extcache (antememoria externa)
- 5 = hod client cache (Host On-Demand 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. Si se selecciona la modalidad de puerto 3 (`cache=3`), consulte el Capítulo 12, “Configuración y supervisión de la Antememoria de servidor Web” en la página 201 para obtener más información sobre la Antememoria de servidor Web.
2. Si se selecciona la modalidad de puerto 5 (`hod client cache=5`), consulte el Capítulo 10, “Configuración y supervisión de Host On-Demand Client Cache para eNetwork de IBM” en la página 151 para obtener más información sobre la Antememoria de servidor Web.

reach *dirección*

Especifica las direcciones de sistema principal a las que el Network Dispatcher debe poder acceder para funcionar correctamente. Pueden ser la dirección de un servidor, de un direccionador, de una estación de administración o de otro sistema principal IP.

dirección

Especifica la dirección IP destino.

Valores válidos: Cualquier dirección IP

Valor por omisión: 0.0.0.0

Ejemplo:

```
add reach
Address to reach [0.0.0.0]?
```

server *dirección-cluster núm-puerto dirección-servidor peso-servidor estado-servidor*

Especifica los atributos de un servidor en un cluster.

dirección-cluster

Especifica la dirección IP del cluster al que pertenece el servidor.

Valores válidos: Cualquier dirección IP

Valor por omisión: 0.0.0.0

núm-puerto

Especifica el protocolo que ejecuta la conexión con este servidor.

Valores válidos: de 1 a 65535

Valor por omisión: 80

dirección-servidor

Especifica la dirección IP del servidor.

Valores válidos: Cualquier dirección IP

Valor por omisión: 0.0.0.0

peso-servidor

Especifica el peso del servidor para el ejecutor. Esto afecta a la frecuencia con que el Network Dispatcher envía solicitudes a este servidor concreto.

Valores válidos: de 0 hasta el valor del *peso-máx* especificado en el mandato add port.

Valor por omisión: peso-máx especificado en el mandato add port

estado-servidor
Especifica si el ejecutor debe considerar el servidor como disponible o como no disponible, cuando aquél empiece a procesar.

Valores válidos: 0 (inactivo) o 1 (activo)

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 a la configuración de parámetros

En la Tabla 14 se listan los límites de las distintas opciones que pueden configurarse para un Network Dispatcher.

Tabla 14. Límites a la configuración de parámetros

Parámetro	Límite
Asesores	8 por cada 2212
Clusters	32 por cada 2212
Latidos	8 por cada 2212
Puertos	8 por cluster
Accesos	8 por cada 2212
Servidores	32 por cada puerto configurado, 128 por cada número de puerto correspondiente a todos los clusters configurados.
Dirección IP del servidor exclusiva	32 por cada 2212

Clear

Utilice el mandato **clear** para borrar toda la configuración del Network Dispatcher.

Sintaxis:

clear

Disable

Utilice el mandato **disable** para inhabilitar un componente del Network Dispatcher.

Sintaxis:

disable advisor . . .
backup
executor
manager

advisor *nombre núm-puerto*
Inhabilita un asesor del Network Dispatcher.

nombre

Especifica el tipo de asesor.

Para obtener más información, consulte la Tabla 13 en la página 122.

Valores válidos: de 0 a 7

Valor por omisión: 0

núm-puerto

Especifica el número de puerto del asesor.

Valores válidos: de 1 a 65535

Valor por omisión: Ninguno. Debe escribir un número de puerto.

Ejemplo:

```
disable 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
```

backup

Inhabilita la función de reserva del Network Dispatcher.

Ejemplo:

```
disable backup
Backup is now disabled.
```

executor

Inhabilita el ejecutor del Network Dispatcher. Al inhabilitar el ejecutor se inhabilita la característica Network Dispatcher.

Ejemplo:

```
disable executor
Executor is now disabled.
```

Nota: Al inhabilitar el ejecutor se parará el gestor, los asesores y la función de alta disponibilidad, en caso de que estuvieran ejecutándose.

manager

Inhabilita el gestor del Network Dispatcher. El gestor es un componente opcional. Sin embargo, si no utiliza el gestor, Network Dispatcher repartirá la carga según un método de planificación rotativo, basado en los pesos actuales de los servidores.

Ejemplo:

```
disable manager
Manager is now disabled.
```

Nota: Puesto que el componente gestor es requisito previo para el funcionamiento de los asesores, si se inhabilita el gestor, se detendrá el funcionamiento de todos los gestores.

Enable

Utilice el mandato **enable** para habilitar un componente del Network Dispatcher.

Sintaxis:

enable advisor . . .

backup

executor

manager

advisor *nombre núm-puerto*

Habilita un asesor para el Network Dispatcher.

nombre

Especifica el tipo de asesor.

Para obtener más información, consulte la Tabla 13 en la página 122.

Valores válidos: de 0 a 7

Valor por omisión: 0

núm-puerto

Especifica el número de puerto del asesor.

Valores válidos: de 1 a 65535

Valor por omisión: Ninguno. Debe escribir 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: Como el componente gestor es requisito previo para el funcionamiento del asesor, debe habilitarse el gestor antes de poder habilitar los asesores. Al configurar los pesos del servidor, utilizados para tomar decisiones sobre el reparto de la carga, también deberá definir las proporciones del gestor para que el gestor tenga en cuenta las entradas de los asesores. Para que el asesor funcione correctamente, también deberá definir la dirección ip interna con el mandato **set internal-ip-address**. Consulte el capítulo Configuración y supervisión IP, de *Configuración y supervisión de protocolos - Manual de consulta Volumen 1* para obtener más información sobre el mandato **set internal-ip-address**.

backup

Habilita la función de reserva del Network Dispatcher.

Ejemplo: `enable backup`

Nota: Antes de habilitar la función de reserva, deberá añadir al menos un latido

executor

Habilita el ejecutor del Network Dispatcher.

Ejemplo:

```
enable executor
Executor is now enabled.
```

manager

Habilita el gestor del 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.
```

Al habilitar el gestor por primera vez, se crea un registro del gestor con los valores por omisión siguientes:

Intervalo: 2 segundos

Ciclo de renovación: 2

Sensibilidad: 5 %

Corrección: 1.5

Proporciones:

- **Activas:** 50%
- **Nuevas:** 50%
- **Asesor:** 0
- **Sistema:** 0

Consulte el mandato “Set” en la página 135 para obtener una descripción de los parámetros que aparecen más arriba.

List

Utilice el mandato **list** para visualizar información sobre el Network Dispatcher.

Sintaxis:

list all | advisor | backup | cluster | manager | port | server

all Muestra toda la información de configuración del Network Dispatcher. Esto incluye a los asesores, función de reserva, clusters, gestor, puertos y servidores.

Ejemplo:

Configuración de Network Dispatcher

```
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
Muestra la configuración de los asesores del Network Dispatcher.

backup
Muestra la configuración de la función de reserva para el Network Dispatcher.

cluster Muestra la configuración de los clusters del Network Dispatcher.

manager
Muestra la configuración del gestor del Network Dispatcher.

port Muestra la configuración de los puertos del Network Dispatcher.

server Muestra la configuración de los servidores asociados con los clusters del 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 *nombre núm-puerto*

Elimina un asesor determinado de la configuración de Network Dispatcher.

nombre

Especifica el tipo de asesor.

Para obtener más información, consulte la Tabla 13 en la página 122.

Valores válidos: de 0 a 7

Valor por omisión: 0

núm-puerto

Especifica el número de puerto del asesor.

Valores válidos: de 1 a 65535

Valor por omisión: Ninguno. Debe escribir un número de puerto.

Ejemplo:

```
remove advisor
Advisor name (0=ftp,1=http,2=MVS,3=TN3270,4=smtp,5=nntp,6=pop3,7=telnet) [0]?
Advisor port [0]? 80
```

backup

Elimina la función de alta disponibilidad.

Nota: Puesto que la función de reserva es requisito previo para las funciones de latido y de acceso, si se elimina la función de reserva, se detendrá el funcionamiento de las funciones de latido y de acceso.

Ejemplo: `remove backup`

cluster *dirección*

Elimina un cluster de la configuración de Network Dispatcher.

dirección

Especifica la dirección IP del cluster.

Valores válidos: Cualquier dirección IP

Valor por omisión: 0.0.0.0

Nota: Al eliminar una dirección de cluster también se eliminan todos los puertos y servidores asociados con 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 *dirección*

Elimina la dirección de latido de la configuración de Network Dispatcher.

Configuración de Network Dispatcher

dirección

Especifica la dirección IP del Network Dispatcher de destino.

Valores válidos: Cualquier dirección IP

Valor por omisión: 0.0.0.0

Ejemplo:

```
remove heartbeat
Target address [0.0.0.0]? 131.2.25.92
```

port *dirección-cluster núm-puerto*

Elimina un puerto de un cluster determinado de la configuración de Network Dispatcher.

dirección-cluster

Especifica la dirección IP del cluster.

Valores válidos: Cualquier dirección IP.

Valor por omisión: 0.0.0.0

núm-puerto

Especifica el número de puerto del protocolo para este cluster.

Valores válidos: de 1 a 65535

Valor por omisión: Ninguno. Debe escribir un número de puerto.

Notas:

1. Al eliminar un puerto también se eliminarán todos los servidores asociados con dicho puerto.
2. Si la modalidad del puerto es la de antememoria, también se eliminará la configuración del Proxy de la Antememoria de servidor Web asociado.
3. Si la modalidad del puerto que se va a eliminar es la de Host On-Demand Client Cache, también se eliminará la configuración del Proxy de Host On-Demand Client Cache.

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 *dirección*

Elimina un servidor de la lista de sistemas principales a los que el Network Dispatcher debe poder acceder.

dirección

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 *dirección-cluster núm-puerto dirección-servidor*

Elimina un servidor de un cluster y puerto de la configuración del Network Dispatcher.

dirección-cluster
Especifica la dirección IP del cluster.

Valores válidos: Cualquier dirección IP.

Valor por omisión: 0.0.0.0

núm-puerto
Especifica el número de puerto del protocolo para este cluster.

Valores válidos: de 1 a 65535

Valor por omisión: Ninguno. Debe escribir un número de puerto.

dirección-servidor
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 asesor, cluster, puerto o servidor ya existentes. También puede definir atributos para el gestor del Network Dispatcher.

Sintaxis:

set advisor . . .
cluster . . .
manager . . .
port . . .
server . . .

advisor *nombre núm-puerto intervalo tiempo-espera puerto-com*
Cambia el número de puerto, intervalo y tiempo de espera de un asesor.

nombre
Especifica el tipo de asesor.

Para obtener más información, consulte la Tabla 13 en la página 122.

Valores válidos: de 0 a 7

Valor por omisión: 0

núm-puerto
Especifica el número de puerto del asesor.

Valores válidos: de 1 a 65535

Valor por omisión: Ninguno. Debe escribir un número de puerto.

intervalo
Especifica la frecuencia con que el asesor consulta a su protocolo para cada servidor. Transcurrida la mitad del intervalo sin obtener

respuesta por parte del servidor, el asesor considera que el protocolo no está disponible.

Valores válidos: de 0 a 65535

Valor por omisión: 5

tiempo de espera
Especifica el intervalo de tiempo, en segundos, después del cual el asesor considera que el protocolo no está disponible.

Para asegurarse de que el gestor no utiliza información desfasada en las decisiones que debe tomar sobre el reparto de la carga, el gestor no utilizará la información suministrada por el asesor cuya indicación de la hora sea anterior a la hora definida en este parámetro. El tiempo de espera del asesor debe ser mayor que el intervalo de sondeo del asesor. Si el tiempo de espera es menor, el gestor no hará caso de los informes que debe utilizar. Por omisión, los informes del asesor no tienen tiempo de espera.

Lo normal es que se utilice este valor si se inhabilita un asesor. No confunda este parámetro con el tiempo de espera de la mitad del intervalo descrito antes, que tiene que ver con la falta de respuesta de un servidor.

Valores válidos: de 0 a 65535

Valor por omisión: 0, lo que significa que se considera que el protocolo siempre está disponible.

puerto-com
Especifica el número de puerto utilizado por el asesor TN3270 para comunicarse con los servidores TN3270. Este parámetro es sólo de entrada para el asesor TN3270.

Valores válidos: de 1 a 65535

Valor por omisión: 10008

Ejemplo:

```
set advisor
Advisor name (0=ftp,1=http,2=MVS,3=TN3270,4=smtp,5=nntp=6=pop3,7=telnet) [0]?
Port number [0]? 21
Interval (seconds) [5]? 10
Timeout (0=unlimited) [0]? 20
```

cluster *dirección cuenta-FIN tiempo-espera-FIN temporizador-inactividad*
Cambia la cuenta de FIN, el tiempo de espera de FIN y el temporizador de inactividad de un cluster en la configuración de Network Dispatcher.

dirección
Especifica la dirección IP del cluster.

Valores válidos: Cualquier dirección IP

Valor por omisión: 0.0.0.0

cuenta de FIN
Especifica el número de conexiones que deben estar en el estado FIN antes de que el ejecutor intente eliminar la información de conexión no usada de la base de datos del Network Dispatcher después de transcurrido el *tiempo de espera de FIN* o el definido en el *temporizador de inactividad*.

Valores válidos: de 0 a 65535

Valor por omisión: 4000

tiempo de espera de FIN
Especifica el número de segundos que han de transcurrir antes de que el ejecutor intente eliminar la información de conexión no usada de la base de datos de Network Dispatcher.

Valores válidos: de 0 a 65535

Valor por omisión: 30

Temporizador de inactividad
Especifica el número de segundos que una conexión puede permanecer inactiva, antes de que el ejecutor intente 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:

```
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 *intervalo proporción renovación sensibilidad corrección*
Define los valores que el gestor utiliza para determinar qué servidor satisfará mejor una petición.

intervalo
Especifica, en segundos, el tiempo que transcurrirá antes de que el gestor actualice los pesos del servidor que utiliza el ejecutor para repartir el reparto de cargas de las conexiones.

Valores válidos: de 0 a 65535

Valor por omisión: 2

proporción
Especifica la importancia relativa de factores externos en las decisiones que toma el gestor sobre pesos. La suma de las proporciones debe ser igual a 100. Los factores son los siguientes:

activo (active)
Número de conexiones activas en cada servidor TCP/IP, al que le sigue la pista el ejecutor.

Valores válidos: de 0 a 100

Valor por omisión: 50

nuevas
Número de conexiones nuevas en cada servidor TCP/IP, conocido por el ejecutor.

Valores válidos: de 0 a 100

Valor por omisión: 50

asesor Entrada de los asesores de protocolo definida para Network Dispatcher.

Valores válidos: de 0 a 100

Valor por omisión: 0

sistema (system)
Entrada del asesor del sistema MVS proporcionada por la herramienta de supervisión del sistema WLM de MVS.

Valores válidos: de 0 a 100

Valor por omisión: 0

renovación
Especifica la frecuencia con que el gestor solicita al ejecutor que le informe sobre el estado. Este parámetro se especifica como un número de *intervalos*.

Valores válidos: de 0 a 100

Valor por omisión: 2

sensibilidad
Especifica el cambio en el porcentaje de los pesos de todos los servidores de un puerto, después del cuál, el gestor actualiza los pesos que utiliza el ejecutor para repartir la carga de las conexiones.

Valores válidos: de 0 a 100

Valor por omisión: 5

corrección
Especifica un límite al peso que puede cambiar un servidor. La corrección minimiza la frecuencia con que se producen los cambios en la distribución de peticiones. Un índice de corrección más alto hará que los pesos cambien menos a menudo. Un índice de corrección más bajo hará que los pesos cambien más a menudo.

Valores válidos: valor decimal entre 1,0 y 42 949 673,00

Valor por omisión: 1,5

Nota: Sólo pueden especificarse dos números decimales.

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 *dirección-cluster núm-puerto tipo-puerto peso-máx modalidad-puerto*
Cambia el tipo de puerto, el peso máximo y la modalidad del puerto para un cluster y número de puerto determinados.

dirección-cluster
Especifica la dirección IP del cluster.

Valores válidos: Cualquier dirección IP.

Valor por omisión: 0.0.0.0

núm-puerto
Especifica el número de puerto del protocolo para este cluster.

Valores válidos: de 1 a 65535

Valor por omisión: Ninguno. Debe escribir un número de puerto.

tipo-puerto
Especifica el tipo de tráfico IP cuya carga puede repartirse en este puerto.

Valores válidos:

tcp=1

upd=2

ambos=3

Valor por omisión: 3

peso-máx
Especifica el peso para los servidores de este puerto. Esto afecta a la diferencia que habrá en el número de peticiones que el ejecutor entregará a cada servidor.

Valores válidos: de 0 a 100

Valor por omisión: 20

modalidad-puerto
Especifica si el puerto enviará todas las peticiones de un único cliente a un único cliente (llamado adherente), utilizará ftp pasivo (pftp), utilizará la Antememoria de servidor Web (antememoria), las enviará a un conjunto de antememorias escalables externas, utilizará Host On-Demand Client Cache, o no utilizará ningún protocolo para este cluster (ninguno).

Valores válidos:

none (ninguna)=0

sticky (adherente)=1

pftp=2

cache (antememoria)=3

extcache (antememoria externa)=4

hod client cache (Host On-Demand Client Cache)=5

Valor por omisión: 0 (ninguna)

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. Si se selecciona la modalidad de puerto 3 (cache=3), consulte el Capítulo 12, “Configuración y supervisión de la Antememoria de servidor Web” en la página 201 para obtener información sobre la Antememoria del servidor Web.
2. Si se selecciona la modalidad de puerto 5 (hod client cache=5), consulte el Capítulo 10, “Configuración y supervisión de Host On-Demand Client Cache para eNetwork de IBM” en la página 151 para obtener más información sobre la Antememoria del servidor Web.

server *dirección-cluster núm-puerto dirección-servidor peso estado*

Cambia el estado y el peso de un servidor concreto de un cluster.

dirección-cluster
Especifica la dirección IP del cluster al que pertenece el servidor.

Valores válidos: Cualquier dirección IP

Valor por omisión: 0.0.0.0

núm-puerto
Especifica el número de puerto del protocolo para este cluster.

Valores válidos: de 1 a 65535

Valor por omisión: Ninguno. Debe escribir un número de puerto.

dirección-servidor
Especifica la dirección IP del servidor.

Valores válidos: Cualquier dirección de servidor válida

Valor por omisión: 0.0.0.0

estado Especifica si el ejecutor debe considerar el servidor como disponible o como no disponible, cuando aquél empiece a procesar.

Valores válidos: 0 (inactivo) o 1 (activo)

Valor por omisión: 1

peso Especifica el peso del servidor para el ejecutor. Esto afecta a la frecuencia con que el Network Dispatcher envía peticiones a este servidor concreto.

Valores válidos: 0 hasta el valor del *peso-máx* especificado en el mandato add port.

Valor por omisión: peso-máx especificado en el mandato add 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 del Network Dispatcher

Para acceder al entorno de supervisión del Network Dispatcher:

1. Escriba **talk 5** en el indicador OPCON (*).
2. Escriba **feature ndr** en el indicador GWCON (+).

El Network Dispatcher también puede supervisarse mediante SNMP. Para obtener más información, consulte el apartado " Gestión SNMP", de la publicación *Configuración y supervisión de protocolos - Manual de consulta Volumen 1*.

Mandatos de supervisión del Network Dispatcher

En la Tabla 15 se resumen todos los mandatos de supervisión del Network Dispatcher y el resto del apartado se dedica a explicar los mandatos. Entre los mandatos en el indicador `NDR >`.

Tabla 15. Mandatos de supervisión de Network Dispatcher

Mandato	Función
? (Ayuda)	Visualiza todos los mandatos disponibles para este nivel de mandato, o lista las opciones de mandatos específicos (si es que están disponibles). Consulte "Obtención de ayuda" en la página xxv.
List	Muestra los atributos configurados actualmente para el asesor, clusters, puertos o servidores.
Quiesce	Especifica que no se deben enviar más peticiones de conexión a un servidor. Además, detiene temporalmente las funciones de latido y acceso.
Report	Muestra un informe sobre el asesor y el gestor.
Status	Muestra el estado actual de los contadores, clusters, puertos, servidores, asesor, gestor y función de reserva.
Switchover	Obliga a un Network Dispatcher que se está ejecutando en modalidad de espera a convertirse en el Network Dispatcher activo. Este mandato es necesario utilizarlo si se ha especificado que la modalidad de intercambio es manual.
Unquiesce	Permite al gestor del Network Dispatcher asignar un peso mayor que 0 a un servidor previamente desactivado en cada puerto para el que está configurado el servidor. Esta acción permite enviar nuevas peticiones de conexión al servidor seleccionado.
Exit	Hace volver al nivel de mandato anterior. Consulte "Salida de un entorno de nivel inferior" en la página xxv.

List

Utilice el mandato **list** para visualizar información sobre el Network Dispatcher.

Sintaxis:

list advisor
cluster
port
server

advisor

Muestra la configuración de los asesores del 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 Muestra la configuración de los clusters del 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 Muestra la configuración de los puertos del Network Dispatcher.

Ejemplo:

```
list port
Cluster Address [0.0.0.0]? 131.2.25.91

  ----------------------------------------------------------
   CLUSTER:       131.2.25.91
  ----------------------------------------------------------
     PORT        MAXWEIGHT      PORT MODE     PORT TYPE
  ----------------------------------------------------------
       23             30          none           TCP
       80             20          none           both
 ----------------------------------------------------------
```

server Muestra la configuración de los servidores asociados con los clusters del 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 parar temporalmente las funciones de latido o de acceso, o para especificar que no deben enviarse más peticiones de conexión a un servidor.

Sintaxis:

quiesce heartbeat
manager
reach

heartbeat *dirección*

Detiene la vía elegida para la función de latido. La *dirección* es la dirección IP del Network Dispatcher remoto al que envía mensajes de Latido este Network Dispatcher.

Ejemplo:

```
quiesce heartbeat
Remote Address [0.0.0.0]? 131.2.25.94
```

manager *dirección*

Especifica que no deben hacerse más peticiones de conexión al servidor especificado. *Dirección* es la dirección IP del servidor.

Ejemplo:

```
quiesce manager
Server Address [0.0.0.0]? 131.2.25.93
```

reach *dirección*

Detiene el sondeo que realiza el Network Dispatcher en la dirección especificada para determinar si es accesible, donde la *dirección* es la dirección IP que forma parte de los criterios de accesibilidad.

Ejemplo:

```
quiesce reach
Reach Address [0.0.0.0]? 131.2.25.92
```

Report

Utilice el mandato **report** para ver un informe sobre el asesor o sobre el gestor.

Sintaxis:

report advisor
manager

advisor *tipo núm-puerto*
Muestra un informe sobre un asesor determinado.

tipo El tipo de asesor. En la Tabla 13 en la página 122 se listan los tipos de asesores.

núm-puerto
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
Muestra un informe sobre la información actual del 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 asesores, función de reserva, contador, clusters, gestor, puertos y servidores.

Sintaxis:

st**atus**
- advisor
- backup
- cluster
- counter
- manager
- ports
- servers

advisor *nombre núm-puerto*

Obtiene el estado de un asesor determinado.

nombre

Especifica el tipo de asesor. En la Tabla 13 en la página 122 se listan los tipos de asesores.

núm-puerto

El número de puerto.

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 reserva.

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 *dirección*

Obtiene el estado de un cluster determinado, donde la *dirección* 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 *dirección-cluster núm-puerto*

Obtiene el estado de un puerto determinado, donde:

dirección-cluster
: es la dirección IP del cluster.

núm-puerto
: es el número de puerto del 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 *dirección*

Obtiene el estado de un servidor determinado, donde la *dirección* es la dirección IP del cluster al que pertenece el servidor.

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 está ejecutando en modalidad de espera a convertirse en el Network Dispatcher activo cuando la estrategia de intercambio es manual. Este mandato debe entrarse en el sistema principal donde se está ejecutando el Network Dispatcher que está en modalidad de espera.

Sintaxis:

sw**itchover**

Unquiesce

Utilice el mandato **unquiesce** para reiniciar un gestor o una función de latido o de acceso detenidos previamente con el mandato **quiesce**.

Sintaxis:

u**nquiesce** heartbeat
manager
reach

heartbeat *dirección*
Reinicia la vía para los mensajes de Latidos, donde *dirección* es la dirección IP del network dispatcher remoto al que este Network Dispatcher está enviando mensajes de Latidos.

Ejemplo:

```
unquiesce heartbeat
Remote Address [0.0.0.0]? 9.10.11.1
```

manager *dirección*
Reinicia el envío de peticiones de conexión al servidor especificado. *Dirección* es la dirección IP del servidor.

Ejemplo:

```
unquiesce manager
Server Address [0.0.0.0]? 20.21.22.15
```

reach *dirección*

Reinicia el sondeo que realiza el Network Dispatcher en la dirección especificada para determinar si es accesible, donde la *dirección* es la dirección IP que forma parte de los criterios de accesibilidad.

Ejemplo:

```
unquiesce reach
Reach address [0.0.0.0]? 20.3.4.5
```

Capítulo 10. Configuración y supervisión de Host On-Demand Client Cache para eNetwork de IBM

Host On-Demand Client Cache permite a los clientes basados en Web conectarse a aplicaciones de sistemas principales SNA mediante un programa de emulación de terminal basado en Java, que conecta el cliente con el sistema principal mediante TN3270. Este soporte permite que un IBM 2212 actúe como servidor TN3270E para guardar en antememoria el applet de emulación de terminal y pueda servir a las peticiones de los navegadores de los clientes. El applet se recupera de un Servidor Web la primera vez que un cliente lo solicita, se almacena en memoria y está disponible para los clientes que envíen una petición `HTTP get` del applet.

Notas:

1. Las características Host On-Demand Client Cache y antememoria del servidor Web no pueden coexistir en una configuración.
2. La característica Host On-Demand Client Cache sólo funciona en la Tarjeta del sistema de alto rendimiento.

En este capítulo se describe cómo configurar la característica Host On-Demand Client Cache y cómo utilizar los mandatos de supervisión de dicha característica. Consta de los apartados siguientes:

- "Configuración de Host On-Demand Client Cache"
- "Acceso al entorno de configuración de Host On-Demand Client Cache" en la página 155
- "Mandatos de Host On-Demand Client Cache" en la página 155
- "Acceso al entorno de supervisión de Host On-Demand Client Cache" en la página 159
- "Mandatos de supervisión de Host On-Demand Client Cache" en la página 159.

En el apartado "Visión general del gestor de control de antememoria externa" en la página 174 hallará información sobre la utilización del Gestor de control de antememoria externa, que funciona conjuntamente con Host On-Demand Client Cache.

Configuración de Host On-Demand Client Cache

Host On-Demand Client Cache debe utilizarse con Network Dispatcher. Antes de utilizar por primera vez Host On-Demand Client Cache, deberá:

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.

A continuación podrá utilizar los mandatos de configuración y supervisión para modificar el entorno de Host On-Demand Client Cache.

Nota: Mientras que los cambios realizados en Network Dispatcher a través de Talk 6 modifican la configuración actual en funcionamiento, los cambios realizados en Host On-Demand Client Cache no modifican la configuración actual en funcionamiento a menos que se active explícitamente a través del mandato **activate** en Talk 6 o mediante la característica HOD Client Cache a través de Talk 5. La excepción a esto es que si se elimina mediante la característica NDR a través de Talk 6, un cluster o puerto de un Proxy HTTP, también se eliminará de la configuración actual en funcionamiento el Proxy HTTP de Host On-Demand Client Cache.

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 ofrece una lista de los parámetros del ejemplo, descritos brevemente.

cluster-address
Especifica la dirección IP del cluster.

Nota: Se supone que las direcciones IP del cluster están en la misma subred lógica que el direccionador de saltos anterior (direccionador IP).

Valores válidos: Cualquier dirección IP válida

Valor por omisión: 0.0.0.0

FIN-count Especifica el número de conexiones que deben estar en el estado FIN antes de que el ejecutor intente eliminar la información de conexión no usada de la base de datos de Network Dispatcher después de transcurrido el *tiempo de espera de FIN* o el definido en el *temporizador de inactividad*.

Valores válidos: de 0 a 65535

Valor por omisión: 4000

FIN-timeout Especifica el número de segundos que una conexión puede permanecer en el estado de FIN antes de que el ejecutor intente eliminar la información de conexión no usada 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 puede permanecer inactiva antes de que el ejecutor intente 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: de 1 a 65535

Valor por omisión: 80

port-type Especifica los tipos de tráfico IP cuya carga puede repartirse 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 para los servidores de este puerto. Esto afectará al diferente número de peticiones que el ejecutor entregará a cada servidor.

Valores válidos: de 0 a 100

Valor por omisión: 20

port-mode Especifica si el puerto enviará todas las peticiones de un único cliente a un único servidor (llamado adherente), utilizará ftp pasivo (pftp), las enviará a un conjunto de antememorias escalables externas (antememoria externa), utilizará la función Host On-Demand Client Cache o no utilizará ningún protocolo concreto para este cluster (ninguno).

Valores válidos: 0,1,2,4,5, donde:

- 0 = none (ninguna)
- 1 = sticky (adherente)
- 2 = pftp
- 4 = extcache (antememoria externa)
- 5 = hod client cache (Host On-Demand Client Cache)

Valor por omisión: 0

Configuración y supervisión de Host On-Demand Client Cache

Default server TCP connection timeout
Especifica el tiempo que transcurrirá antes de que finalice la conexión con un servidor.

Valores válidos: de 5 a 240 segundos

Valor por omisión: 120 segundos.

Default client TCP connection timeout
Especifica el tiempo que transcurrirá antes de que finalice la conexión con un cliente.

Valores válidos: de 5 a 240 segundos

Valor por omisión: 120 segundos.

Do you want to modify Host On-Demand Client Cache partition?
Le permite modificar la configuración de la partición de Host On-Demand Client Cache.

Valores válidos: Yes (Sí) o No

Valor por omisión: No

Maximum partition size
Especifica la cantidad máxima de memoria que se asignará a esta partición de Host On-Demand Client Cache. Si este valor es superior a la cantidad de memoria disponible actualmente, se hará caso omiso del valor y no se impondrá ningún tamaño máximo de la partición.

Valores válidos: de 1 a 4095 Megabytes o 0 (sin máximo)

Valor por omisión: 0 (sin máximo)

URL mask to identify Java applets
Especifica la máscara de URL utilizada para identificar los applets Java.

Valores válidos: cualquier máscara de URL

Valor por omisión: *.jar*

Default expiration time for Java applet
Especifica el tiempo de caducidad que se aplicará a los applet Java.

Valores válidos: de 1 a 10080 minutos, o 0 si no caduca

Valor por omisión: 60

Do you want to add a URL mask?
Especifica una máscara de URL nueva que se añadirá a Host On-Demand Client Cache. Las máscaras de URL permiten que el usuario incluya o excluya objetos individuales o grupos de objetos por su Localizador universal de recursos (URL).

Valores válidos: Yes (Sí) o No

Valor por omisión: No

Cuando se especifica una máscara de URL, se pueden utilizar caracteres comodín. Al configurar Network Dispatcher para Host On-Demand Client Cache o al utilizar los mandatos **add** o **modify url** desde el indicador `HOD Client Cache`, pueden utilizarse caracteres comodín. Los caracteres utilizados como comodines son el *

(asterisco) y el # (signo de número). Los comodines pueden utilizarse en cualquier posición del URL.

El signo * indica que o ningún carácter o cualquier número de caracteres forman parte del URL:

Ejemplo: *abc.html filtrará las máscaras de URL siguientes.

```
abc.html
finabc.html
defchtjqsprabc.html
```

El signo # representa un solo carácter.

Ejemplo: ab#.html filtrará las máscaras de URL siguientes.

```
abc.html
abf.html
abo.html
```

Debe utilizar Network Dispatcher para configurar el cluster y puerto iniciales de la característica Host On-Demand Client Cache. Una vez añadidos el cluster y el puerto, al configurar la *modalidad de puerto* como puerto de Host On-Demand Client Cache, podrá modificar y visualizar los parámetros de configuración de Host On-Demand Client Cache en el indicador `HOD Client Cache Config>`.

Consulte 126 para obtener más información sobre Network Dispatcher.

Acceso al entorno de configuración de Host On-Demand Client Cache

Para acceder al entorno de configuración de Host On-Demand Client Cache, escriba el mandato **f hod client cache** en el indicador `Config>`.

```
Config> f h
HOD Client Cache Config>
```

Mandatos de Host On-Demand Client Cache

En este apartado se describen los mandatos de configuración de Host On-Demand Client Cache. En la Tabla 16 se listan los mandatos de configuración de Host On-Demand Client Cache. Estos mandatos especifican los parámetros de la característica Host On-Demand Client Cache. Para activar las modificaciones, reinicie el direccionador.

Tabla 16. Resumen de los mandatos de configuración de Host On-Demand Client Cache

Mandato	Función
? (Ayuda)	Visualiza todos los mandatos disponibles para este nivel de mandato, o lista las opciones de mandatos específicos (si es que están disponibles). Consulte “Obtención de ayuda” en la página xxv.
Activate	Activa la partición de Host On-Demand Client Cache, 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 Host On-Demand Client Cache.
Modify	Modifica la información de Host On-Demand Client Cache.
Exit	Hace volver al nivel de mandato anterior. Consulte “Salida de un entorno de nivel inferior” en la página xxv.

Activate

Utilice el mandato **activate** para inicializar todas las particiones de Host On-Demand Client Cache, utilizando la configuración más reciente.

Sintaxis:

ac**tivate**

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:

ad**d** urlmask

Ejemplo:

```
HOD Client Cache Config>add url
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 proxies y particiones, deberá 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:

de**lete** partition
urlmask

partition
Suprime la partición de Host On-Demand Client Cache.

urlmask
Nombre de la máscara de URL que se suprimirá de Host On-Demand Client Cache.

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 el cluster asociados, o cambiar la modalidad de puerto a otra distinta de Host On-Demand Client Cache.

List

Utilice el mandato **list** para listar la información de Host On-Demand Client Cache.

Sintaxis:

list all
external
partition
proxy
urlmask

all Lista la partición, todos los puertos, proxies y máscaras definidos en una antememoria Host On-Demand Client.

external
Lista la información del Gestor de control de antememoria externa.

partition
Lista la partición de Host On-Demand Client Cache.

proxy Lista los proxies de Host On-Demand Client Cache.

urlmask
Lista las máscaras de URL definidas en Host On-Demand Client Cache.

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.
```

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 Host On-Demand Client Cache.

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 Host On-Demand Client Cache existente.

proxy Cambia las características de un proxy HTTP existente.

urlmask
Cambia una máscara de URL ya 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 Host On-Demand Client Cache

Para acceder al entorno de supervisión de Host On-Demand Client Cache, escriba el mandato **f hod client cache** en el indicador de configuración `t 5`.

```
+f h
```

Mandatos de supervisión de Host On-Demand Client Cache

En la Tabla 17 se listan los mandatos de supervisión de Host On-Demand Client Cache.

Tabla 17. Resumen de mandatos de supervisión de Host On-Demand Client Cache

Mandato	Función
? (Ayuda)	Visualiza todos los mandatos disponibles para este nivel de mandato, o lista las opciones de mandatos específicos (si es que están disponibles). Consulte “Obtención de ayuda” en la página xxv.
Activate	Activa la información de Host On-Demand Client Cache, utilizando la configuración más reciente.
Clear	Borra todos los objetos de la partición de Host On-Demand Client Cache o borra las estadísticas de Host On-Demand Client Cache.
Enable	Habilita la partición de Host On-Demand Client Cache.
Delete	Suprime la partición, el proxy o un máscara de URL de Host On-Demand Client Cache.
Disable	Inhabilita la partición de Host On-Demand Client Cache.
List	Lista la información de Host On-Demand Client Cache.
Modify	Modifica la información de Host On-Demand Client Cache.
Exit	Hace volver al nivel de mandato anterior. Consulte “Salida de un entorno de nivel inferior” en la página xxv.

Activate

Utilice el mandato **activate** para activar la partición, o los proxies o un proxy en concreto de Host On-Demand Client Cache.

Sintaxis:

ac**tivate** all
ex**t**ernal
pa**r**tition
pr**o**xy

all Activa la partición de Host On-Demand Client Cache, todos los proxies definidos y el Gestor de control de antememoria externa.

external
Activa el Gestor de control de antememoria externa.

partition
Activa la partición de Host On-Demand Client Cache.

proxy Activa un proxy de Host On-Demand Client Cache.

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 Host On-Demand Client Cache, o para borrar las estadísticas.

Nota: Al borrar los objetos de la partición, no se borran 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 Host On-Demand Client Cache.

Sintaxis:

enable partition

Ejemplo:

```
HOD Client Cache>enable partition
```

Delete

Utilice el mandato **delete** para suprimir la partición de Host On-Demand Client Cache.

Sintaxis:

delete partition

partition
Suprime la partición de Host On-Demand Client Cache.

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 Host On-Demand Client Cache.

Sintaxis:

disable partition

Ejemplo:

```
HOD Client Cache>disable partition
```

List

Utilice el mandato **list** para visualizar la información de Host On-Demand Client Cache, todas las políticas y proxies, o una política o proxy en concreto.

Sintaxis:

list
all
delete
depend
external
item
partition
policy
proxy

all Lista la partición de Host On-Demand Client Cache, todas las políticas y todos los proxies.

delete Lista los 100 últimos elementos suprimidos de la partición de Host On-Demand Client Cache.

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 de la partición de Host On-Demand Client Cache.

partition
Lista la información de la partición de Host On-Demand Client Cache.

policy Lista la información de las políticas de Host On-Demand Client Cache.

proxy Lista la información de los proxies de Host On-Demand Client Cache.

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
'/futbol.html' -- 2
'/tenis.html' -- 1
'/curling.html' -- 3
```

Ejemplo: list dependency

```
HOD Client Cache>list depend
Dependency table for Partition 0
------------------------------------
dep: tenis_info
   count of URLs: 2
   URLs:
         tenis_roster.html
         tenis_schedule.html
dep: futbol_info
   count of URLs: 2
   URLs:
         futbol_roster.html
         futbol_schedule.html
dep: schedule
   count of URLs: 2
   URLs:
         tenis_schedule.html
         futbol_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
'/archiv5k.html' -- 1
'/archiv4k.html' -- 1
'/archiv2k.html' -- 3
'/archiv1k.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
```

Configuración y supervisión de Host On-Demand Client Cache

Capítulo 11. Utilización de la Antememoria de servidor Web

En este capítulo se describe la función Antememoria de servidor Web del 2212. Consta de los apartados siguientes:

- "Visión general de la Antememoria de servidor Web"
- "Utilización del Proxy HTTP" en la página 170
- "Antememoria escalable de alta disponibilidad" en la página 172
- "Visión general del gestor de control de antememoria externa" en la página 174.

Visión general de la Antememoria de servidor Web

La función de almacenamiento en antememoria del servidor Web sólo está disponible para los modelos 2212 que disponen de la Tarjeta del sistema de alto rendimiento. Los modelos 2212 que no disponen de la Tarjeta del sistema de alto rendimiento pueden actualizarse. Para obtener más información, póngase en contacto con el representante de IBM.

La función de almacenamiento en antememoria del servidor Web almacena la páginas web solicitadas con más frecuencia, para poder recuperarlas más rápidamente. La función de almacenamiento en antememoria del servidor Web mantiene más cerca de los clientes los elementos solicitados con más frecuencia; esto libera recursos del servidor que está siendo utilizado actualmente como servidor de archivos y de conexiones de comunicaciones. La Antememoria de servidor Web del 2212 permite acceder a gran velocidad a las páginas web, reduciendo la actividad general de comunicaciones del sistema principal. La Antememoria de servidor Web del 2212:

- Almacena las páginas web estáticas y que no están protegidas
- Permite que los clientes y servidores HTTP accedan a la antememoria
- Permite que el usuario defina las políticas de llenado y anulación.
- Utiliza la función Network Dispatcher para repartir la carga de trabajo entre los servidores y permite la posibilidad de utilizar una antememoria de reserva.
- Proporciona una plataforma para futuras funciones de almacenamiento en antememoria controladas por el servidor.

Nota: Las funciones antememoria del servidor Web y Host On-Demand Client Cache no pueden coexistir en una configuración.

Todas las interfaces de red del 2212 que dan soporte a la conectividad TCP/IP, dan soporte a la conectividad entre la antememoria del servidor Web y los servidores y clientes HTTP.

La Figura 10 en la página 166 muestra cómo funciona Network Dispatcher sin la función de almacenamiento en antememoria del servidor Web.

Utilización de la Antememoria de servidor Web

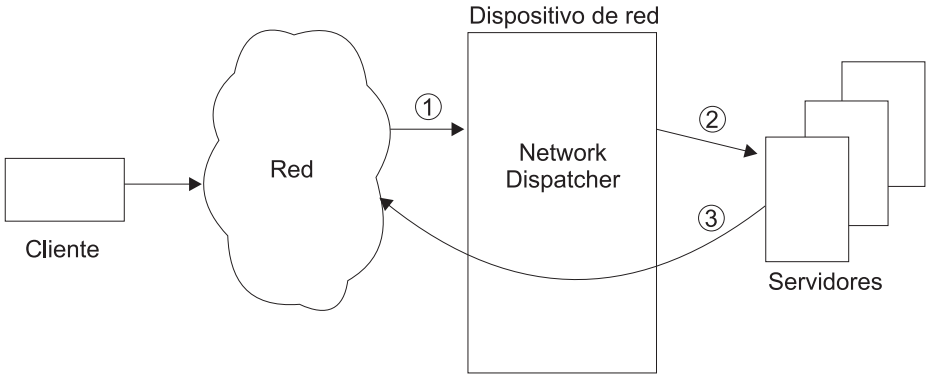


Figura 10. Network Dispatcher sin Antememoria de servidor Web

1. Se solicita una dirección de cluster
2. Network Dispatcher reenvía la petición a los servidores
3. El servidor envía una respuesta al cliente.

La Figura 11 muestra cómo funciona Network Dispatcher con la función de almacenamiento en antememoria del servidor Web. La función de almacenamiento en antememoria del servidor Web carga la respuesta en la antememoria si las políticas lo permiten.

Consulte el apartado “Utilización del Proxy HTTP” en la página 170 para obtener más información sobre el Proxy HTTP.

Una partición es una división del núcleo de la antememoria. Cada partición de la antememoria se particiona a su vez, permitiendo que el dispositivo dé soporte a varios clusters.

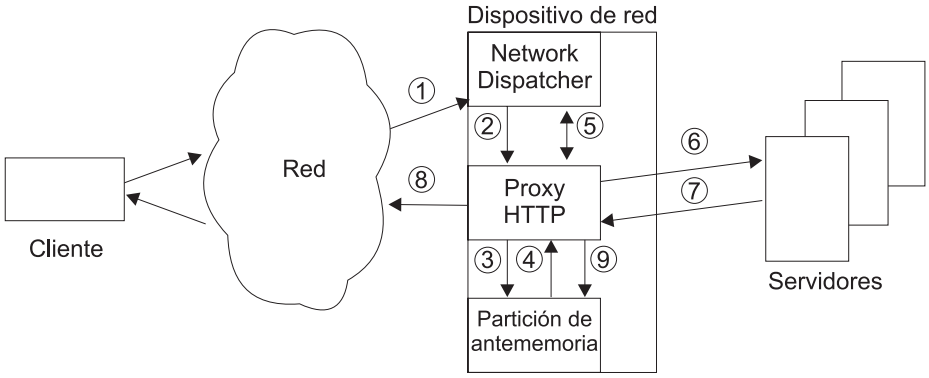


Figura 11. Network Dispatcher con Antememoria de servidor Web y sin acierto en la antememoria

1. Se solicita una dirección de cluster
2. Network Dispatcher reenvía la petición al Proxy HTTP, si está activo
3. El Proxy HTTP busca en 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 la información del servidor desde Network Dispatcher, si es necesaria para una nueva conexión
6. El Proxy HTTP reenvía la petición al servidor. (Para la conexión TCP la dirección IP origen es la dirección de la interfaz de red del 2212. La dirección IP destino es la dirección IP de la interfaz del servidor).

7. El servidor envía la 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 la función de almacenamiento en antememoria del servidor Web cuando la página solicitada está actualmente almacenada en antememoria.

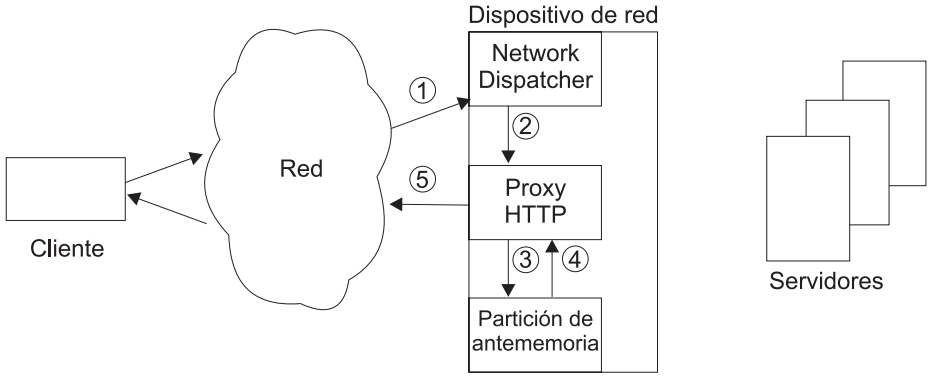


Figura 12. Network Dispatcher con Antememoria de servidor Web y con acierto en la antememoria

1. Se solicita una dirección de cluster
2. Network Dispatcher reenvía la petición al Proxy HTTP
3. El Proxy HTTP busca en 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.

Almacenamiento en antememoria

La Antememoria de servidor Web del 2212 tiene:

Almacenamiento en antememoria de páginas web

El 2212 puede almacenar en antememoria objetos que solicita el servidor. Este método de almacenamiento en antememoria se conoce como almacenamiento transparente en antememoria. Puede utilizar `talk 6` para habilitar o inhabilitar el almacenamiento transparente en antememoria en una partición.

La alternativa al almacenamiento transparente en antememoria (automático) es el almacenamiento manual en antememoria. Es esta caso, un agente externo maneja el gestor de antememoria para almacenar en antememoria una página web. Para obtener más información sobre el almacenamiento en antememoria externa de páginas web, consulte el apartado “Visión general del gestor de control de antememoria externa” en la página 174.

Los objetos almacenados en antememoria inactivos se suprimen automáticamente. La Antememoria de servidor Web del 2212 da soporte a servidores y clientes HTTP 1.0 y 1.1.

Políticas flexibles de almacenamiento en antememoria

Permite que los usuarios especifiquen si deben almacenarse en antememoria determinadas clases genéricas de objetos web (imágenes, páginas estáticas que no son imágenes, páginas dinámicas). También se pueden especificar los tamaños máximos de los objetos y de las particiones de la antememoria. Además, los usuarios pueden especificar máscaras de URL para incluir o excluir explícitamente clases de objetos web según convenga en su entorno.

Diagrama de flujo de las políticas de almacenamiento transparente en antememoria

1. ¿Están habilitados el almacenamiento en antememoria y el almacenamiento transparente en antememoria?
   - No - El objeto no se almacenará en antememoria.
   - Sí - Continuar con la próxima comprobación.
2. ¿El tamaño del objeto es menor o igual que el tamaño máximo?
   - No - El objeto no se almacenará en antememoria.
   - Sí - Continuar con la próxima comprobación.
3. ¿El objeto ha caducado?
   - No - Continuar con la próxima comprobación.
   - Sí - El objeto no se almacenará en antememoria.
4. ¿Van a utilizarse encabezamientos HTTP y se ha utilizado uno de ellos?

   Nota: El encabezamiento HTTP utilizado es un encabezamiento de control de la antememoria on las directivas DO o DONT.

   a. No - ¿No se van a utilizar encabezamientos HTTP o el objeto no tiene encabezamiento?
      1) ¿El URL está excluido por una máscara de exclusión?
         - Sí - El objeto no se almacenará en antememoria.
         - No - Continuar con la próxima comprobación.
      2) ¿El URL está incluido mediante una máscara de inclusión?
         - Sí - Ir al paso 5 en la página 169.
         - No - Continuar con la próxima comprobación.
      3) ¿Es un objeto dinámico?
         - No - Continuar con la próxima comprobación.
         - Sí - El objeto es dinámico.

           1. ¿Los objetos dinámicos deben almacenarse en antememoria?

           — Sí - Continuar con la próxima comprobación.

           — No - El objeto no se almacenará en antememoria.
      4) ¿El objeto es una imagen (.jpg o .gif)?
         - No - Continuar con la próxima comprobación.

- Sí - El objeto es una imagen.

  1. ¿Las imágenes deben almacenarse en antememoria?

  — Sí - Continuar con la próxima comprobación.

  — No - El objeto no se almacenará en antememoria.

5) ¿El objeto es estático y no es una imagen?
   - No - Continuar con la próxima comprobación.
   - Sí - El objeto es un archivo estático y no es una imagen.

     1. ¿Los objetos estáticos y que no son una imagen deben almacenarse en antememoria?

     — Sí - Continuar con la próxima comprobación.

     — No - El objeto no se almacenará en antememoria.

b. Sí - ¿Se utilizan encabezamientos HTTP y el objeto incluye un encabezamiento de control de la antememoria?
   1) ¿Los encabezamientos HTTP contienen la directiva "DO"?
      a) No - El objeto no se almacenará en antememoria.
      b) Sí - Continuar con la próxima comprobación.

5. ¿Hay espacio en la partición para almacenar el objeto?

   Nota: Los objetos utilizados menos recientemente se eliminarán para dejar sitio al objeto.

   - No - El objeto no se almacenará en antememoria.
   - Sí - El objeto se almacenará en antememoria.

Soporte de varias antememorias independientes
Se da soprte a un máximo de 16 particiones, lo que permite a un solo 2212 proporcionar servicios de almacenamiento en antememoria independientes para varios clusters. Las particiones de la antememoria son totalmente independientes. Cada partición de la antememoria posee contenido y políticas propios.

Conectividad total del servidor TCP/IP
Comunica los servidores y los clientes entre todas las interfaces de red del 2212 que dan soporte al conjunto de protocolos TCP/IP.

Reparto de la carga de los servidores finales (utilizando Network Dispatcher)
Utiliza Network Dispatcher para definir grupos de servidores y repartir la carga entre los servidores para acelerar la búsqueda de páginas web que no se han encontrado en la antememoria.

Soporte de antememoria de reserva
Permite que los usuarios definan un segundo 2212 como antememoria del servidor de reserva. La antememoria del servidor de reserva puede funcionar como reserva "en frío" utilizando la función de Alta disponibilidad de Network Dispatcher. Hallará más información en “Alta disponibilidad de Network Dispatcher” en la página 107.

Nota: Al activarse, la antememoria del servidor de reserva está vacía. Para volver a llenar de páginas la antememoria del servidor de reserva deberá utilizar el almacenamiento transparente en antememoria (por ejemplo: peticiones de URL) o la función gestor de control de antememoria externa.

Utilización del Proxy HTTP

Puede haber más de un Proxy HTTP en el 2212. Cada uno representa una dirección o un puerto de cluster dedicado al almacenamiento en antememoria. Pueden existir varios proxies HTTP utilizando una partición de la antememoria.

El Proxy HTTP maneja las peticiones recibidas de los clientes e intenta satisfacerlas desde su partición de la antememoria. Si el Proxy HTTP puede satisfacer la petición, devolverá la respuesta al cliente. Si el Proxy HTTP no puede satisfacer la petición, abrirá una conexión TCP con un servidor para intentar satisfacerla. Cuando el servidor responda a la petición del Proxy HTTP, éste reenviará al cliente la respuesta del servidor. El Proxy HTTP también decide si la respuesta del cliente debe almacenarse en antememoria. SI la respuesta debe almacenarse en antememoria, el Proxy HTTP la pasa a la partición de la antememoria.

El Proxy HTTP maneja las conexiones siguiendo estas directrices.

- El Proxy HTTP intentará satisfacer solamente las peticiones de métodos GET y HEAD desde la antememoria. Las otras peticiones se enviarán al servidor sin modificaciones a través de una conexión TCP con el servidor que está conectado con la conexión TCP del cliente. Si ninguna conexión TCP está conectada con la conexión TCP del cliente, se abrirá una nueva conexión TCP con el servidor y se conectará con la conexión TCP del cliente.
- Los mensajes de todas las peticiones de métodos GET y HEAD que no puedan satisfacerse desde la partición de la antememoria, se enviarán al servidor sin modificaciones a través de la conexión TCP.
- Todas las respuestas recibidas del servidor se volverán a enviar al cliente sin modificaciones a través de la conexión TCP con el cliente.
- Únicamente se almacenarán en antememoria las respuestas del método GET. Se considera que las otras respuestas no deben almacenarse en antememoria. Las respuestas GET se almacenarán en antememoria solamente si el estado de la respuesta es aceptable, y la respuesta GET y las políticas de almacenamiento en antememoria para la partición lo permiten.
  - Sólo se almacenarán en antememoria las respuestas con los códigos de estado siguientes: El Proxy HTTP no permitirá que los encabezamientos HTTP anulen esto.

    Códigos de estado:
    - 200 (ok)
    - 203 (non-authoritative)
    - 300 (multiple-choice)
    - 301 (moved permanently)
    - 410 (gone)
- Si se utilizan encabezamientos HTTP en una petición GET, el encabezamiento de petición `If-Modified-Since` es el único que se utilizará para determinar si una entrada de la antememoria puede satisfacer la petición. No se utilizará ningún otro encabezamiento condicional. La Antememoria de servidor Web no

utilizará identificadores de entidad para determinar si una entidad almacenada en antememoria puede utilizarse como respuesta.

- Se hace caso omiso de las directivas de encabezamiento `control de la antememoria` incluidas en las peticiones. Si la entidad no está en la partición de la antememoria, la petición se pasa al servidor.

  Nota: La Antememoria de servidor Web es una extensión del servidor y, por lo tanto, no utiliza el encabezamiento `Control de la antememoria` como las antememorias del Proxy HTTP.

- Las respuestas dan soporte a las directivas de encabezamiento de la antememoria "do" y "dont". Se hace caso omiso de las otras directivas.Las directivas "do" y "dont" son directivas nuevas que puede utilizar el servidor para informar a la Antememoria de servidor Web de que almacene la entidad en antememoria o de que no lo haga.

  Nota: La Antememoria de servidor Web es una extensión del servidor y, por lo tanto, no utiliza el encabezamiento `Control de la antememoria` como las antememorias del Proxy HTTP.

- El Proxy HTTP intenta satisfacer peticiones GET parciales desde la antememoria. Sin embargo, las respuestas GET parciales no se almacenan en la antememoria.

  Nota: Si una petición GET parcial tiene más de diez rangos, se devolverá la respuesta completa.

- Se hará caso omiso del encabezamiento `Host` de todos los mensajes HTTP, puesto que todas las peticiones de entrada deben ser para el mismo cluster de servidores.
- El Proxy HTTP da soporte a conexiones HTTP continuas.

  Nota: Si se recibe una conexión continua de un cliente de nivel HTTP 1.0 y se devuelve respuesta desde la antememoria, se añadirá un encabezamiento `Connection` dependiendo de la petición. Por ejemplo, si el cliente quiere que la duración de la conexión sea larga, se mantendrá una conexión larga.

- El Proxy HTTP no utilizará la antememoria para las peticiones que contengan el encabezamiento `Authorization`. No se almacenarán en antememoria las respuestas a dichas peticiones. Tampoco se almacenarán en antememoria las respuestas que tengan un encabezamiento `Proxy-Authorization`.
- El Proxy HTTP será capaz de pasar a un comportamiento de transmisión a través de un túnel para una conexión HTTP, si tiene problemas analizando una petición o una respuesta de una conexión HTTP. El comportamiento de transmisión a través de un túnel para todos los análisis de mensajes y reenvía todas las peticiones del cliente al servidor y todas las respuestas del servidor al cliente.
- Si la partición de la antememoria está inhabilitada, todas las conexiones actuales y nuevas de clientes se reenviarán directamente al servidor final.
- Si Ia partición de la antememoria está habilitada, la antememoria procesará todas las conexiones nuevas de clientes. Las conexiones ya existentes de clientes continuarán reenviando las peticiones directamente al servidor final.

Antememoria escalable de alta disponibilidad

La antememoria escalable de alta disponibilidad permite que un grupo de antememorias de servidor Web trabajen como una sola antememoria más grande. El número máximo de antememorias que pueden formar parte de un grupo es de dieciséis. Si se produce una anomalía en un miembro de la antememoria, se reduce la cantidad total de memoria disponible para almacenar datos en antememoria, en lugar de finalizar todas las funciones de almacenamiento en antememoria. En la Figura 9 en la página 119 encontrará un ejemplo de configuración.

Las antememorias individuales forman el espacio total de la antememoria. Si una antememoria deja de funcionar, las otras antememorias en funcionamiento continuarán almacenando en antememoria las páginas de entrada.

Las páginas web de entrada se almacenan en las antememorias del grupo. Se distribuyen equitativamente entre las antememoria disponibles. Cada antememoria del grupo mantiene una tabla que hace un seguimiento del número de antememorias accesibles del grupo y de sus direcciones IP. Las tablas son idénticas para todas las antememorias del grupo. Las tablas utilizan un algoritmo llamado protocolo de rutinas para un conjunto de antememorias (CARP, Cache Array Routine Protocol) para determinar en qué antememoria se guarda un URL determinado. La información de la tabla se obtiene del dispositivo Network Dispatcher e, indirectamente, de las antememorias que utilizan el asesor HTTP para realizar el seguimiento del estado de las antememorias de servidor Web del grupo. Las figuras siguientes demuestran las condiciones para localizar un URL utilizando la SHAC.

La Figura 13 muestra la petición recibida de Network Dispatcher encontrada en la primera antememoria que ha recibido la petición.

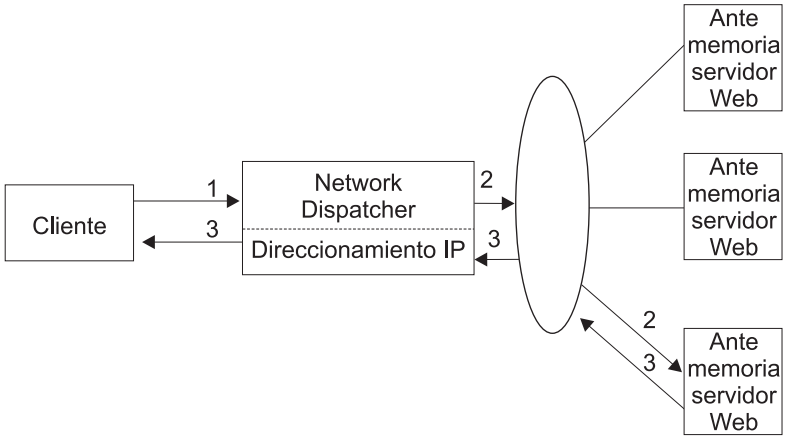


Figura 13. Encontrada petición hecha a la antememoria

1. Llega al Network Dispatcher una petición HTTP de una página web realizada por un cliente.
2. Network Dispatcher reenvía la petición a una de las antememorias de servidor Web. La antememoria recibe la petición y encuentra la página web.
3. La antememoria envía la página web directamente al cliente, evitando Network Dispatcher.

La Figura 14 en la página 173 muestra una petición recibida de Network Dispatcher que no se ha encontrado en la primera antememoria, pero que el algoritmo CARP indica que el URL se guarda en otra antememoria.

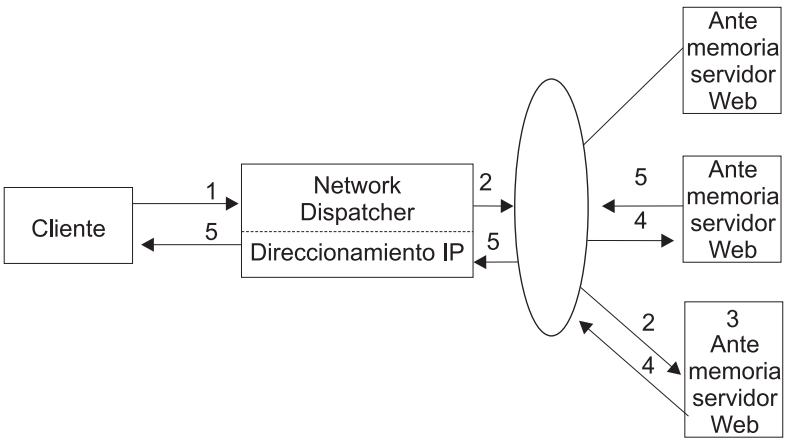


Figura 14. Petición reenviada a la antememoria responsable

1. Llega al Network Dispatcher una petición HTTP de una página web realizada por un cliente.
2. Network Dispatcher reenvía la petición a una de las antememorias de servidor Web.
3. La antememoria recibe la petición y no encuentra la página web. Como consecuencia, la antememoria utiliza un algoritmo para localizar la antememoria responsable de la página web.
4. A continuación, la petición se reenvía a la antememoria responsable de esta página web.
5. La antememoria responsable de la página web recibe la petición, encuentra la página web y se la envía al cliente.

La Figura 15 muestra una petición recibida de Network Dispatcher que no se ha encontrado en la antememoria, pero el algoritmo CARP indica que la antememoria es responsable del URL.

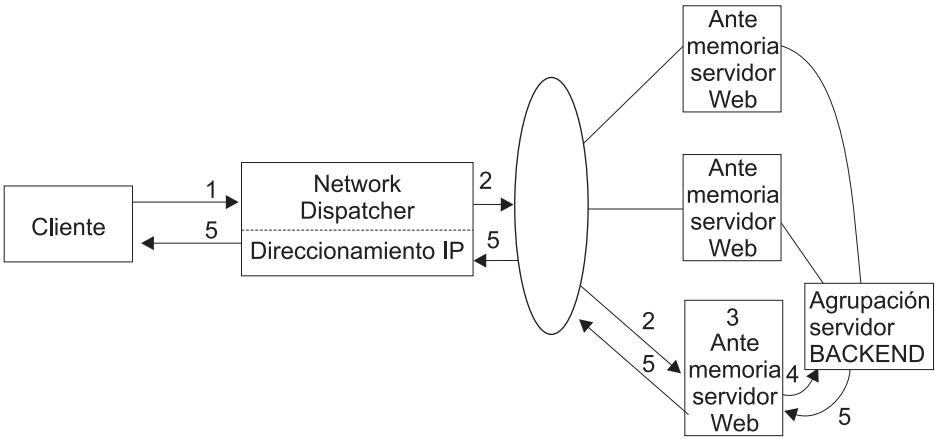


Figura 15. Petición reenviada al servidor final

1. Llega al Network Dispatcher una petición HTTP de una página web realizada por un cliente.
2. Network Dispatcher reenvía la petición a una de las antememorias de servidor Web.

3. La antememoria recibe la petición y no encuentra la página web. La antememoria utiliza un algoritmo para determinar cuál es la antememoria responsable de la página web.
4. La antememoria envía la petición al servidor final.
5. El servidor final encuentra la página web; dicha página se devuelve al cliente a través de la antememoria responsable de la página. Se almacenará en antememoria si ésta está configurada para almacenar la página en antememoria. Consulte el Capítulo 12, “Configuración y supervisión de la Antememoria de servidor Web” en la página 201 para obtener información sobre la configuración.

La Figura 16 muestra una petición que no se ha encontrado en ninguna antememoria del grupo de antememorias.

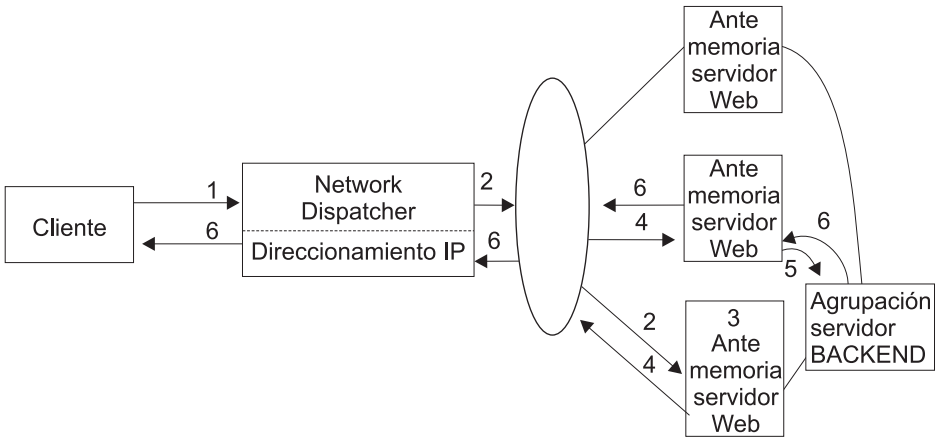


Figura 16. Petición reenviada a la antememoria responsable y no encontrada

1. Llega al Network Dispatcher una petición HTTP de una página web realizada por un cliente.
2. Network Dispatcher reenvía la petición a una de las antememorias de servidor Web.
3. La antememoria recibe la petición y no encuentra la página web. Como consecuencia, la antememoria utiliza un algoritmo para localizar la antememoria responsable de la página web. A continuación, la petición se reenvía a la antememoria responsable de esta 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 servidores finales.
6. El servidor final encuentra la página web; dicha página se devuelve al cliente a través de la antememoria responsable de la página. Se almacenará en antememoria si ésta está configurada para almacenar la página en antememoria. Consulte el Capítulo 12, “Configuración y supervisión de la Antememoria de servidor Web” en la página 201 para obtener información sobre la configuración.

Visión general del gestor de control de antememoria externa

El gestor de control de antememoria externa permite que los Servidores Web controlen la antememoria del servidor Web y la antememoria Host On-Demand Client. El control se consigue a través de un puerto definido por el usuario para el

gestor de control de antememoria externa (ECCM, External Cache Control Manager). El ECCM acepta mandatos de conexiones y de procesos con destino a una partición de este puerto. Los mandatos utilizan el protocolo de control de la antememoria externa (ECCP, External Cache Control Protocol). El ECCP utiliza formatos de vectores y subvectores para enviar mandatos de petición y mandatos de respuesta.

Un vector de mandatos puede solicitar varias funciones utilizando varios subvectores. Cada subvector representa una función diferente. El vector de mandatos indica en qué partición de la antememoria se aplicarán los mandatos, para lo que debe especificar la dirección del cluster y el puerto de un proxy definido para esa partición.

El ECCP da soporte a las funciones siguientes:

- Añadir un objeto a una partición de la antememoria, así como suprimirlo
- Habilitar o inhabilitar una partición de la antememoria
- Modificar o listar las políticas aplicables a la partición de la antememoria
- Borrar o listar las estadísticas de la partición de la antememoria
- Borrar una partición de la antememoria (eliminar todos los objetos de la partición de la antememoria)
- Consultar la partición de la antememoria (buscar un objeto determinado)
- Añadir, suprimir, listar o borrar las máscaras de URL de una partición de la antememoria
- Modificar o listar la tabla de dependencias
- Anular objetos que utilizan dependencias.

Tabla de dependencias

El gestor de control de antememoria externa le permite crear una tabla de dependencias para cada partición de la antememoria. Esta tabla es particularmente útil cuando se trabaja con objetos dinámicos en la antememoria.

Nota: Almacenar objetos dinámicos en antememoria requiere que los objetos se actualicen cuando se modifica la información a partir de la que se crearon dichos objetos.

La información necesaria para crear la tabla de dependencias debe pasarse a la partición de la antememoria mediante la interfaz del gestor de control de antememoria externa.

La tabla de dependencias le ofrece la posibilidad de asignar una serie de dependencias a un objeto URL (página web almacenada en antememoria). Estas dependencias se almacenan en tablas de dependencias de la antememoria del servidor Web mediante la interfaz del gestor de control de antememoria externa. La tabla de dependencias se utiliza para anular objetos de la partición de la antememoria cuando se modifica el origen del objeto. Sin una tabla de dependencias, habría que enviar un mandato de suprimir individual para cada objeto que se quisiera suprimir.

Ejemplo: Las tres bases de datos siguientes contienen varios objetos.

```
basedatos1          basedatos2          basedatos3
---------           ---------           ---------
objeto_a            objeto_a            objeto_b
objeto_b            objeto_c            objeto_e
objeto_c            objeto_d
```

Supongamos que todas las páginas objeto_a a objeto_e están almacenadas en la antememoria. Si la base de datos 2 cambia, se puede enviar (a través de la interfaz del gestor de control de la antememoria) un mandato **invalid dependency basedatos2**. Como consecuencia, la antememoria del servidor Web suprimirá los objetos objeto_a, objeto_c y objeto_d de la partición de la antememoria.

Nota: Un objeto no tiene que estar en la partición de la antememoria para estar en la tabla de dependencias.

Autenticación del gestor de control de antememoria externa

El gestor de control de antememoria externa le permite controlas el acceso de los usuarios. Esto se consigue al solicitar a las conexiones de entrada una identificación de usuario y una contraseña. La identificación de usuario y la contraseña están ligadas con la identificación de usuario y la contraseña de conexión. Si el dispositivo está protegido por una contraseña y la conexión de entrada no tiene identificación de usuario ni contraseña o éstas no son válidas, se devolverá una respuesta de error y se cerrará la conexión. Si la identificación de usuario y la contraseña son válidas, el usuario podrá enviar mandatos a través de la interfaz.

Seguridad

La seguridad proporciona una forma de autenticar el usuario del ECCP. Se pueden configurar cuatro tipos de autenticación (RADIUS, TACACS, local o ninguno). No se proporciona el cifrado de datos. Cada mecanismo de cifrado (excepto ninguno) requiere tanto una identificación de usuario como su contraseña asociada. Esta información se envía al 2216 mediante vectores de autenticación. La identificación de usuario y la contraseña pueden tener de 1 a 8 bytes. La contraseña que se envía por la conexión del Control de la antememoria externa debe cifrarse mediante el método de cifrado DES. También se envía el número generador aleatorio de 8 bytes utilizado para el cifrado. La clave del cifrado no se envía a través de la conexión. En “Modify” en la página 211, hallará información sobre cómo configurar el puerto y los valores TCP.

Nota: Si el direccionador no está protegido mediante contraseña, se hará caso omiso del vector de autenticación.

Protocolo de control de la antememoria externa

El protocolo de control de la antememoria externa (ECCP) proporciona a los servidores finales la capacidad de controlar la antememoria del direccionador. Este control maximiza el rendimiento de la antememoria.

El ECCP es una interfaz construida en forma de protocolo que permite que los servidores añadan y supriman objetos así como que puedan modificar las políticas de la antememoria.

El gestor de control de antememoria externa se define en el direccionador (antememoria del servidor Web o antememoria Host On-Demand Client) de forma que acepte mandatos de conexiones y de procesos con destino a una partición de la antememoria.

Configuración

El gestor de control de antememoria externa se configura con los parámetros siguientes:

Puerto definido por el usuario:
Número de puerto en el que el gestor de control de antememoria externa escucha y acepta conexiones. Si se configura como 0, se supone que el gestor de antememoria externa está inhabilitado.

Valores válidos: de 0 a 65535

Valor por omisión: 0

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 mediante contraseña. La clave de cifrado debe ser una serie de 16 caracteres hexadecimales (0-9,a-f,A-F).

Descripciones de las funciones del gestor de control de antememoria externa

En este apartado se describen las funciones del gestor de control de antememoria externa.

Añadir un objeto

Puede añadirse a la partición de la antememoria un objeto respuesta HTTP. El formato de los datos del objeto debe ser igual al de una respuesta HTTP. El gestor de control de antememoria externa analizará los encabezamientos de la respuesta y extraerá la información necesaria. Es entonces cuando se añadirá el objeto a la antememoria.

La diferencia entre Añadir objeto y Añadir objeto (obligatoriamente) es que éste último mandato hará caso omiso de los encabezamientos Control de antememoria que especifiquen DO o DONT. Se siguen utilizando los demás encabezamientos que utiliza el Proxy HTTP para determinar si almacenar en antememoria un objeto. Ambos mandatos Añadir objeto y Añadir objeto (obligatoriamente) sustituirán el objeto en la partición de la antememoria sin tener en cuenta la fecha.

Suprimir un objeto

Puede suprimirse de la antememoria un objeto HTTP. Se da el URL del objeto.

Utilización de la tabla de dependencias

La tabla de dependencias de una partición de la antememoria puede modificarse, listarse y utilizarse para anular objetos.

Para modificar la tabla de dependencias (añadir o eliminar dependencias), deben incluirse tanto la dependencia como el URL de la dependencia. Además, existen otras dos formas de modificar la tabla de dependencias. Una consiste en restaurar toda la tabla (es decir, eliminar todas las dependencias), o la URL de una dependencia (es decir, eliminar la URL de una dependencia de todas las dependencias). La otra consiste en efectuar un proceso de recogida de basura de la tabla de dependencias. El proceso de recogida de basura borra todos los URL de dependencias de la tabla de dependencias que no tengan ningún objeto con ese URL en la antememoria.

Hay varias maneras de listar la información de la tabla de dependencias. Puede recuperarse toda la tabla, todos los URL de dependencias de una dependencia concreta, o todas las dependencias que tienen un URL de una dependencia dada.

Los objetos pueden eliminarse (anularse) de la antememoria utilizando la Tabla de dependencias. Se comprueba la Tabla de dependencias utilizando la dependencia,. Se eliminarán de la partición de la antememoria, las URL de dependencias de esa dependencia.

Inhabilitar y habilitar una partición

Esta función permite cambiar el estado de la partición de la antememoria. Para poder utilizar el gestor de control de antememoria externa, la partición de la antememoria debe estar en el estado correcto. La partición de la antememoria debe estar inhabilitada para poder depurar los objetos que contiene.

Utilización de las políticas

Las políticas de una partición se pueden listar o modificar. Cada política puede aplicarse independientemente o para todo el grupo. Para modificar una política, debe pasarse el tipo de datos correcto correspondiente a esta política. Consulte el apartado “Formatos de los vectores del protocolo de control de la antememoria externa (ECCP)” en la página 179 (Subvector de mandatos Política y Subvector de respuesta Política) para saber los formatos de los datos dependiendo de cuál es la política.

Depurar la partición

Esta función permite eliminar todos los objetos de la partición de la antememoria. La partición de la antememoria debe estar inhabilitada para poder depurarla.

Consultar un objeto

Esta función permite ver si un objeto está en la partición de la antememoria. Además, si el objeto está en la partición de la antememoria y tiene una fecha de última modificación, se devuelve la fecha. Consulte el apartado “Formatos de los vectores del protocolo de control de la antememoria externa (ECCP)” en la página 179 (Subvector de respuesta Consulta) para saber el formato de la fecha que se devuelve.

Utilización de las estadísticas

Esta función permite listar y restaurar (borrar) las estadísticas de la partición de la antememoria. Consulte el apartado “Formatos de los vectores del protocolo de control de la antememoria externa (ECCP)” en la página 179 (Subvector de respuesta Estadísticas) para saber cuál es el formato de las estadísticas.

Utilización de una máscara de URL

Esta función permite listar y modificar las máscaras de URL de una partición de la antememoria. Cuando se utilice esta función, deberá incluirse el tipo de URL, de inclusión, de exclusión, dinámico o applet Host On-Demand Client Cache. Se debe listar un tipo de URL. Esta función no funciona con varios tipos de URL.

Tiene la posibilidad de añadir una máscara de URL. Si la máscara de URL es de inclusión, dinámica o una máscara del applet Host On-Demand Client Cache, debe incluirse el ciclo de vida. Al añadir una máscara dinámica se modificará la máscara de URL dinámica actual y al añadir una máscara del applet Host On-Demand

Client Cache, se modificará la máscara actual del applet Host On-Demand Client Cache. Tiene la posibilidad de suprimir una máscara de URL. Esta función no es válida para la máscara URL dinámica o para la máscara del applet Host On-Demand Client Cache. Tiene la posibilidad de restaurar todas las máscaras de URL de un tipo concreto. Restaurar una máscara de URL dinámica restaura la máscara de URL dinámica por omisión, y restaurar la máscara del applet Host On-Demand Client Cache restaura la máscara del applet Host On-Demand Client Cache por omisión.

Nota: La máscara dinámica se utiliza con imágenes de la antememoria del servidor Web y la máscara del applet Host On-Demand Client Cache se utiliza con imágenes que tengan la función Host On-Demand Client Cache.

Formatos de los vectores del protocolo de control de la antememoria externa (ECCP)

Los clientes ECCP envían mandatos y reciben respuestas utilizando un formato de vector. El vector de autenticación es necesario si el recuadro está protegido mediante contraseña. Si el recuadro no está protegido mediante contraseña, se hará caso omiso del vector de autenticación si se recibe.

Formatos de los vectores

En este apartado se ofrecen las descripciones de los campos de los vectores.

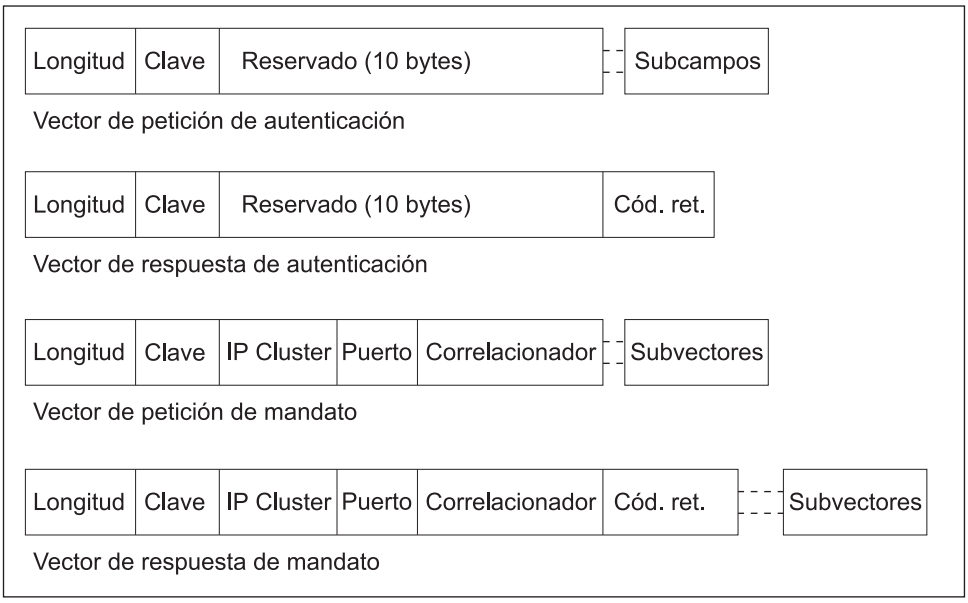


Figura 17. Vector de respuesta de mandatos

Longitud: Valor de 32 bits sin signo que representa la longitud (en bytes) de todo el vector, incluida la de los campos longitud y clave, así como la de los subvectores y subcampos. El rango de valores aceptables está comprendido entre 22 y 4GB para vectores de mandatos, y de 38 a 52 para vectores de autenticación.

Clave: Valor de 16 bits sin signo que representa la clave del vector principal. Las claves del vector principal son:

- 0x4A00 (Vector de petición de autenticación)
- 0x4A01 (Vector de respuesta de autenticación)

- 0x4B00 (Vector de petición de mandatos)
- 0x4B01 (Vector de respuesta de mandatos)

IP del cluster: Dirección IP del cluster de la antememoria asociado con la partición de la antememoria de destino.

Puerto: Número de puerto del cluster de la antememoria asociado con la partición de la antememoria.

Correlacionador: Valor de 32 bits sin signo utilizado por el cliente del ECCP para asociar la respuesta del mandato con la petición del mandato.

Código de retorno: Valor de 32 bits sin signo que representa el código de retorno. Sólo aparece en los vectores de respuesta.

Los vectores contienen uno o más subvectores. El vector de petición de autenticación requiere los subcampos nombre y contraseña. El vector de petición de mandatos contiene uno o más subvectores de mandatos. Si existen varios subvectores en el vector de petición de mandatos, existirán varios subvectores en el vector de respuesta de mandatos. Si se produce un error grave, se reflejará en el campo Código de retorno del vector de respuesta de mandatos.

Vector de petición de autenticación

El Vector de petición de autenticación debe ser el primer vector de la Conexión del control de la antememoria externa, si el recuadro está protegido mediante contraseña. Si el recuadro no está protegido mediante contraseña, se hará caso omiso del vector.

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x4A00

6-15 Reservado

Reservado para su futuro uso.

16-n Subcampo nombre.

n+1-m Subcampo contraseña.

Vector de petición de mandatos

El Vector de petición de mandatos envía mandatos al gestor de control de antememoria externa. Si el recuadro está protegido mediante contraseña, el gestor de control de antememoria externa deberá recibir un Vector de petición de autenticación válido antes de aceptar los mandatos.

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x4B00

6-9 Dirección IP del cluster

Dirección IP de un cluster de antememorias (Proxy HTTP) asociado con la partición de la antememoria de destino.

10-11 Puerto

Número de puerto del cluster de antememorias (Proxy HTTP) asociado con la partición de la antememoria de destino.

12-15 Correlacionador

El correlacionador se utiliza para asociar las respuestas de mandatos con sus correspondientes peticiones de mandatos.

16-n Subvectores

Puede añadirse uno o más de los subvectores siguientes.

- Subvector de mandatos Añadir objeto (0x0100)
- Subvector de mandatos Añadir objeto (obligatoriamente) (0x0110)
- Subvector de mandatos Eliminar objeto (0x0400)
- Subvector de mandatos Dependencia (0x0A00)
- Subvector de mandatos Inhabilitar (0x0300)
- Subvector de mandatos Habilitar (0x0200)
- Subvector de mandatos Política (0x0500)
- Subvector de mandatos Depurar (0x0600)
- Subvector de mandatos Consulta (0x0700)
- Subvector de mandatos Estadísticas (0x0800)
- Subvector de mandatos Máscara de URL (0x900)

Vector de respuesta de autenticación

El Vector de respuesta de autenticación se devuelve en respuesta a un Vector de petición de autenticación.

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x4A01

6-15 Reservado

Reservado para su futuro uso.

16-19 Código de retorno

Código de retorno del vector. Consulte el apartado “Códigos de retorno” en la página 199.

20-n Subvectores

Actualmente no existen subvectores para el Vector de respuesta de autenticación.

Vector de respuesta de mandatos

El Vector de respuesta de mandatos se devuelve en respuesta a un Vector de petición de mandatos.

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x4B01

6-9 Dirección IP del cluster

Dirección IP de un cluster de antememorias (Proxy HTTP) asociado con la partición de la antememoria de destino.

10-11 Puerto

Número de puerto del cluster de antememorias (Proxy HTTP) asociado con la partición de la antememoria de destino.

12-15 Correlacionador

El correlacionador se utiliza para asociar las respuestas de mandatos con sus correspondientes peticiones de mandatos.

16-19 Código de retorno

Código de retorno del vector. Consulte el apartado “Códigos de retorno” en la página 199.

20-n Subvectores

Se puede añadir el número de subvectores siguientes que se quiera, o no añadir ninguno.

- Subvector de respuesta Añadir objeto (0x0101)
- Subvector de respuesta Añadir objeto (obligatoriamente) (0x0111)
- Subvector de respuesta Eliminar objeto (0x0401)
- Subvector de respuesta Dependencia (0x0A01)
- Subvector de respuesta Inhabilitar (0x0301)
- Subvector de respuesta Habilitar (0x0201)
- Subvector de respuesta Política (0x0501)
- Subvector de respuesta Depurar (0x0601)
- Subvector de respuesta Consulta (0x0701)
- Subvector de respuesta Estadísticas (0x0801)
- Subvector de respuesta Máscara de URL (0x901)

Formatos de los subvectores

En este apartado se describen los formatos de los subvectores. Los subvectores tienen básicamente el mismo formato que el vector principal:

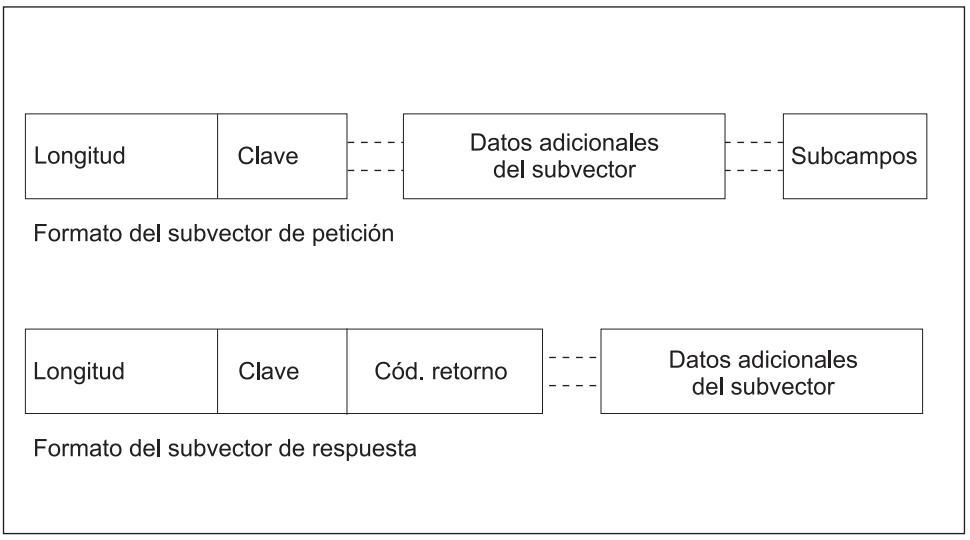


Figura 18. Formato de un subvector

Longitud: Valor de 32 bits sin signo que representa la longitud (en bytes) de todo el subvector, incluida la de los campos longitud y clave, así como la de los subcampos. El rango de valores aceptables está comprendido entre 6 y 4GB (no se comprueba el límite superior).

Clave: Valor de 16 bits sin signo que representa la clave del subvector. Las claves de los subvectores de petición son las siguientes:

- 0x0100 (Añadir un objeto WEB)
- 0x0110 (Añadir un objeto WEB, haciendo caso omiso de los encabezamientos de control de la antememoria)
- 0x0200 (Habilitar el almacenamiento en la antememoria de la partición)
- 0x0300 (Inhabilitar el almacenamiento en la antememoria de la partición)
- 0x0400 (Eliminar un objeto WEB)
- 0x0500 (Modificar o listar las políticas de la antememoria)
- 0x0600 (Eliminar todos los objetos WEB de la partición)
- 0x0700 (Determinar si un objeto WEB está en la partición)
- 0x0800 (Restaurar o listar las estadísticas de la antememoria)
- 0x0900 (Añadir, suprimir o listar las máscaras de URL)
- 0x0A00 (Añadir, suprimir, listar o restaurar dependencias)

Las claves de los subvectores de respuesta que se devuelven son las siguientes:

- 0x0101 (Añadir un objeto WEB)
- 0x0111 (Añadir un objeto WEB, haciendo caso omiso de los encabezamientos de control de la antememoria)
- 0x0201 (Habilitar el almacenamiento en la antememoria de la partición)
- 0x0301 (Inhabilitar el almacenamiento en la antememoria de la partición)
- 0x0401 (Eliminar un objeto WEB)
- 0x0501 (Modificar o listar las políticas de la antememoria)
- 0x0601 (Eliminar todos los objetos WEB de la partición)
- 0x0701 (Determinar si un objeto WEB está en la partición)
- 0x0801 (Restaurar o listar las estadísticas de la antememoria)
- 0x0901 (Añadir, suprimir o listar las máscaras de URL)

- 0x0A01 (Añadir, suprimir, listar o restaurar dependencias)

Código de retorno: Valor de 32 bits sin signo que representa el código de retorno del subvector de petición. Sólo aparece en el subvector de respuesta.

Subvector de mandatos Añadir objeto: El Subvector de mandatos Añadir objeto se utiliza para añadir un Objeto Web a la partición de la antememoria.

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x0110

6-n Subcampo URL

n+1-m Subcampo objeto

Subvector de mandatos Añadir objeto (obligatoriamente): El Subvector de mandatos Añadir objeto (obligatoriamente) se utiliza para añadir un Objeto Web a la partición de la antememoria. Se diferencia del Subvector de mandatos Añadir objeto en que se hace caso omiso de los encabezamientos de Control de la antememoria del objeto.

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x0100

6-n Subcampo URL

n+1-m Subcampo objeto

Subvector de mandatos Eliminar objeto: El Subvector de mandatos Eliminar objeto se utiliza para eliminar un Objeto Web de la partición de la antememoria.

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x0400

6-n Subcampo URL

Subvector de mandatos Dependencia: El Subvector de mandatos Dependencia se utiliza para modificar o listar la Tabla de dependencias o para anular objetos utilizando la Tabla de dependencias.

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x0A00

6-7 Mandato

Mandato de dependencia a ejecutar.

0x0001 Obtener la tabla de dependencias (consulte el tipo de Dependencia para la dependencia)

0x0002 Añadir una dependencia o un URL de dependencias nueva a la Tabla de dependencias

0x0003 Eliminar una dependencia o un URL de dependencias de la Tabla de dependencias

0x0004 Restaurar la información de la tabla de dependencias (consulte el tipo de Dependencia para la dependencia)

0x0005 Anular un Objeto según la dependencia

0x0006 Recoger la basura de la Tabla de dependencias

8-9 Tipo de Dependencia

Este campo se utiliza para identificar qué datos deben cambiarse. Estos datos se modifican utilizando el Mandato Dependencia.

0x0000 No existe tipo de dependencia

0x0001 Utilizar el mandato en toda la tabla.

- Si el mandato es 0x0001 (Obtener) - obtiene toda la tabla.
- Si el mandato es 0x0004 (Restaurar) - borra toda la tabla.

0x0002 El mandato se aplica a la dependencia.

- Si el mandato es 0x0001 (Obtener) - obtiene todos los URL de la dependencia dada.
- Si el mandato es 0x0004 (Restaurar) - borra de la tabla una dependencia.

0x0003 El mandato se aplica al URL

- Si el mandato es 0x0001 (Obtener) - obtiene todas las dependencias del URL de dependencias.
- SI el mandato es 0x0004 (Restaurar) - borra de la tabla un URL de dependencias.

10-n Varios subcampos o ninguno.

Subcampo Dependencia
Nota: Este subcampo debe ser el primero, en caso de que se requieran ambos subcampos. Es obligatorio cuando se tienen estos tipos de Mandatos Dependencia.

Mandato	Tipo de dependencia
0x0001	0x0002
0x0002	0x0000
0x0003	0x0000
0x0004	0x0002
0x0005	0x0000

Subcampo URL
Nota: Este subcampo debe ser el segundo, en caso de que se requieran ambos subcampos. Es obligatorio cuando se tienen estos tipos de Mandatos Dependencia.

Mandato	Tipo de dependencia
0x0001	0x0003
0x0002	0x0000
0x0003	0x0000
0x0004	0x0003

Subvector del mandato Inhabilitar: EL Subvector de mandatos Inhabilitar se utiliza para inhabilitar una partición de la antememoria.

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x0300

Subvector de mandatos Habilitar: El Subvector de mandatos Habilitar se utiliza para habilitar una partición de la antememoria.

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x0200

Subvector de mandatos Política: El Subvector de mandatos Política le permite modificar una partición de la antememoria o listar la información de una partición de la antememoria.

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x0500

6-7 Mandato

Mandato a ejecutar.

0x0001 Obtener la política

0x0002 Actualizar la política

8-9 Tipo de política

El Tipo de política se utiliza para identificar los datos que deben cambiarse. A continuación, los datos se cambiarán utilizando el Mandato Política.

0x0001 Almacenamiento transparente en antememoria

0x0002 Encabezamiento HTTP de control de la antememoria

0x0003 Almacenar en antememoria objetos dinámicos

0x0004 Almacenar en antememoria objetos imagen ("*.gif," "*.jpg")

0x0005 Almacenar en antememoria objetos estáticos

0x0006 Ciclo de vida por omisión de los objetos dinámicos

0x0007 Ciclo de vida por omisión de los objetos imagen

0x0008 Ciclo de vida por omisión de los objetos estáticos.

0x0009 Tiempo (en segundos) que transcurrirá entre cada recogida de basura.

0x000A
Tamaño máximo de la partición (en MB).

0x000B
Número máximo de objetos en la partición de la antememoria.

0x000C
Tamaño máximo de un objeto de la partición de la antememoria.

0xFFFF
Operar con todas las políticas.

Nota: **Si el Mandato es Obtener (0x0001), el subvector terminará aquí.**

10-n Uno de los siguientes, dependiendo del Tipo de política.

Si el Tipo de política es 0x0001, 0x0002, 0x0003, 0x0004 ó 0x0005:

10-11 Establecer valor

- 0x0001 (Habilitado)
- 0x0002 (Inhabilitado)

Si el Tipo de política es 0x0006, 0x0007 ó 0x0008

10-13 El valor representa el ciclo de vida del objeto, en minutos.

El valor está comprendido entre 0 y 10.080, donde 0 indica que el objeto no caduca.

Si el Tipo de política es 0x0009

10-13 Valor que representa el intervalo de depuración de la antememoria, en minutos.

El valor está comprendido entre 0 y 720, donde 0 indica que el proceso de recogida de basura está inhabilitado.

Si el Tipo de política es 0x000A

10-11 Valor que representa el tamaño máximo de la partición, en MB. El valor está comprendido entre 0 y 4.095, donde 0 indica que no existe límite.

Nota: El valor no se verifica.

Si la política es 0x000B

10-13 Valor que representa el número máximo de objetos.

El valor está comprendido entre 0 y 100000, donde 0 indica que no existe límite.

Nota: El valor no se verifica.

Si la política es 0x000C

10-13 Valor que representa el tamaño máximo de un objeto en la partición de la antememoria.

El valor está comprendido entre 512 y 300.000; si se especifica 0, significa que no existe límite.

Nota: El valor no se verifica.

Si la política es 0xFFFF

10-11 Almacenamiento transparente en antememoria (Establecer valor)

- 0x0001 (Habilitado)
- 0x0002 (Inhabilitado)

12-13 Encabezamiento HTTP de control de la antememoria (Establecer valor)

- 0x0001 (Habilitado)
- 0x0002 (Inhabilitado)

14-15 Almacenamiento en antememoria de objetos dinámicos (Establecer valor)

- 0x0001 (Habilitado)
- 0x0002 (Inhabilitado)

16-17 Almacenamiento en antememoria de objetos imagen (Establecer valor)

- 0x0001 (Habilitado)
- 0x0002 (Inhabilitado)

18-19 Almacenamiento en antememoria de objetos estáticos (Establecer valor)

- 0x0001 (Habilitado)
- 0x0002 (Inhabilitado)

20-21 Valor que representa el tamaño máximo de la partición, en MB.

El valor está comprendido entre 0 y 4.095, donde 0 indica que no existe límite.

Nota: El valor no se verifica.

20-21 Valor que representa el tamaño máximo de la partición, en MB.

El valor está comprendido entre 0 y 4.095, donde 0 indica que no existe límite.

Nota: El valor no se verifica.

22-25 Valor que representa el número máximo de objetos.

El valor está comprendido entre 0 y 1.000.000, donde 0 indica que no existe límite.

Nota: El valor no se verifica.

26-29 Valor que representa el tamaño máximo de un objeto en una partición de la antememoria.

El valor está comprendido entre 512 y 3.000.000; si se especifica 0, significa que no existe límite.

Nota: El valor no se verifica.

30-33 Valor que representa el ciclo de vida de un objeto dinámico, en minutos.

El valor está comprendido entre 0 y 10.080, donde 0 indica que el objeto no caduca.

Nota: El valor no se verifica.

34-37 Valor que representa el ciclo de vida de un objeto imagen, en minutos.

El valor está comprendido entre 0 y 10.080, donde 0 indica que no existe límite.

Nota: El valor no se verifica.

38-41 Valor que representa el ciclo de vida de un objeto estático, en minutos.

El valor está comprendido entre 0 y 10.080, donde 0 indica que no existe límite.

Nota: El valor no se verifica.

42-45 Valor que representa el intervalo de depuración de la antememoria, en minutos.

El valor está comprendido entre 0 y 720, donde 0 indica que debe habilitarse el proceso de recogida de basura.

Subvector de mandatos Depuración: El Subvector de mandatos Depuración se utiliza para borrar todos los objetos de una partición de la antememoria.

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x0600

Subvector de mandatos Consulta: El Subvector de mandatos Consulta se utiliza para comprobar si un URL dado está en la partición de la antememoria.

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x0700

6-n Subcampo URL

Subvector de mandatos Estadísticas: El Subvector de mandatos Estadísticas se utiliza para obtener o restaurar las estadísticas de una partición de la antememoria.

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x0800

6-7 Mandato

- 0x0001 - Obtiene las estadísticas de la partición de la antememoria.
- 0x0004 - Restaura las estadísticas de la partición de la antememoria.

Subvector de mandatos Máscara de URL: El Subvector de mandatos Máscara de URL se utiliza para listar o modificar las máscaras de URL asociadas con una partición de la antememoria.

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x0900

6-7 Mandato

- 0x0001 - Obtiene las máscaras de URL definidas actualmente (consulte más abajo los Tipos de URL para saber qué tipos de máscaras que se devuelven).
- 0x0002 - Añade la máscara de URL dada (consulte más abajo los Tipos de URL para saber cuál es el tipo de máscara que se va a añadir).
- 0x0003 - Eliminar la máscara de URL dada (consulte más abajo los Tipos de URL para saber cuál es el tipo de máscara que se va a eliminar).

  Nota: Suprimir la máscara de URL dinámica o la máscara del applet Host On-Demand Client, no es una función válida.

- 0x0004 - Restaurar todas las máscaras de URL del Tipo de URL definido a continuación.

8-9 Tipo de URL

- 0x0001 - de inclusión
- 0x0002 - de exclusión
- 0x0003 - dinámico
- 0x0004 - applet Host On-Demand Client

10-13 Ciclo de vida

El valor está comprendido entre 0 y 10.080, donde 0 representa un objeto que no caduca. Sólo lo utiliza el mandato Añadir (0x0002), si el tipo de URL es de inclusión (0x0001), dinámico (0x0003) o el applet Host On-Demand Client (0x0004).

Nota: Si el Mandato es Obtener (0x0001) o Borrar (0x0004), el subvector terminará aquí.

14-n Un subvector de mandatos URL.

Subvector de respuesta Añadir objeto: El Subvector de respuesta Añadir objeto se utiliza para responder a un Subvector de mandatos Añadir objeto (obligatoriamente).

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x0101

6-9 Código de retorno

Consulte los “Códigos de retorno” en la página 199.

Subvector de respuesta Añadir objeto (obligatoriamente): El Subvector de respuesta Añadir objeto (obligatoriamente) se utiliza para responder a un Subvector de mandatos Añadir objeto (obligatoriamente).

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x0111

6-9 Código de retorno

Consulte los “Códigos de retorno” en la página 199.

Subvector de respuesta Eliminar objeto: El Subvector de respuesta Eliminar objeto se utiliza para responder a un Subvector de mandatos Añadir objeto (obligatoriamente).

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x0401

6-9 Código de retorno

Consulte los “Códigos de retorno” en la página 199.

Subvector de respuesta Dependencia: El Subvector de respuesta Dependencia se utiliza para responder a un Subvector de mandatos Dependencia.

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x0A01

6-9 Código de retorno

Consulte los “Códigos de retorno” en la página 199.

10-n Varios subcampos o ninguno.

```
Subcampo Dependencia
Nota: Este subcampo debe ir antes que los Subcampos de mandatos
URL de la dependencia.
Es obligatorio cuando se tienen estos tipos de Mandatos Dependencia.
Para obtener más información, consulte el apartado "Subvector de mandatos Dependencia" en la página 184.

Mandato      Tipo de dependencia
 0x0001          0x0001          Nota: Los Subcampos URL que vayan después
                                       del Subcampo Dependencia son
                                       URL de dependencias de esa
                                       dependencia.
 0x0001          0x0003

Subcampo URL
Nota: Este subcampo debe ser el segundo, en caso de que se requieran ambos subcampos.
         Es obligatorio cuando se tienen estos tipos de Mandatos Dependencia.

Mandato      Tipo de dependencia
 0x0001          0x0001          Nota: El Subcampo Dependencia que va antes
                                       del Subcampo URL indica el
                                       URL de la dependencia.
 0x0001          0x0002
```

Subvector de respuesta Inhabilitar: El Subvector de respuesta Inhabilitar se utiliza para responder al Subvector de mandatos Inhabilitar.

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x0301

6-9 Código de retorno

Consulte los "Códigos de retorno" en la página 199.

Subvector de respuesta Habilitar: El Subvector de respuesta Habilitar se utiliza para responder al Subvector de mandatos Habilitar.

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x0201

6-9 Código de retorno

Consulte los "Códigos de retorno" en la página 199.

Subvector de respuesta Política: El Subvector de respuesta Política se utiliza para responder al Subvector de mandatos Política.

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x0501

6-9 Código de retorno

Consulte los "Códigos de retorno" en la página 199.

Si el Subvector de mandatos Política era PUT (0x0002), el subvector terminará aquí.

10-n Uno de los siguientes, dependiendo del Tipo de política del Subvector de mandatos Política.

Si el Tipo de política es 0x0001, 0x0002, 0x0003, 0x0004 ó 0x0005:

10-11 Establecer valor

- 0x0001 (Habilitado)
- 0x0002 (Inhabilitado)

Si el Tipo de política es 0x0006, 0x0007 ó 0x0008

10-13 El valor representa el ciclo de vida del objeto, en minutos.

El valor está comprendido entre 0 y 10.080, donde 0 indica que el objeto no caduca.

Si el Tipo de política es 0x0009

10-13 Valor que representa el intervalo de depuración de la antememoria, en minutos.

El valor está comprendido entre 0 y 720, donde 0 indica que el proceso de recogida de basura está inhabilitado.

Si el Tipo de política es 0x000A

10-11 Valor que representa el tamaño máximo de la partición, en MB. El valor está comprendido entre 0 y 4.095, donde 0 indica que no existe límite.

Nota: El valor no se verifica.

Si la política es 0x000B

10-13 Valor que representa el número máximo de objetos.

El valor está comprendido entre 0 y 100000, donde 0 indica que no existe límite.

Nota: El valor no se verifica.

Si la política es 0x000C

10-13 Valor que representa el tamaño máximo de un objeto en la partición de la antememoria.

El valor está comprendido entre 512 y 300.000; si se especifica 0, significa que no existe límite.

Nota: El valor no se verifica.

Si la política es 0xFFFF

10-11 Almacenamiento transparente en antememoria (Establecer valor)

- 0x0001 (Habilitado)
- 0x0002 (Inhabilitado)

12-13 Encabezamiento HTTP de control de la antememoria (Establecer valor)

- 0x0001 (Habilitado)
- 0x0002 (Inhabilitado)

14-15 Almacenamiento en antememoria de objetos dinámicos (Establecer valor)

- 0x0001 (Habilitado)
- 0x0002 (Inhabilitado)

16-17 Almacenamiento en antememoria de objetos imagen (Establecer valor)

- 0x0001 (Habilitado)
- 0x0002 (Inhabilitado)

18-19 Almacenamiento en antememoria de objetos estáticos (Establecer valor)

- 0x0001 (Habilitado)
- 0x0002 (Inhabilitado)

20-21 Valor que representa el tamaño máximo de la partición, en MB.

El valor está comprendido entre 0 y 4.095, donde 0 indica que no existe límite.

Nota: El valor no se verifica.

22-25 Valor que representa el número máximo de objetos.

El valor está comprendido entre 0 y 1.000.000, donde 0 indica que no existe límite.

Nota: El valor no se verifica.

26-29 Valor que representa el tamaño máximo de un objeto en una partición de la antememoria.

El valor está comprendido entre 512 y 3.000.000; si se especifica 0, significa que no existe límite.

Nota: El valor no se verifica.

30-33 Valor que representa el ciclo de vida de un objeto dinámico, en minutos.

El valor está comprendido entre 0 y 10.080, donde 0 indica que el objeto no caduca.

Nota: El valor no se verifica.

34-37 Valor que representa el ciclo de vida de un objeto imagen, en minutos.

El valor está comprendido entre 0 y 10.080, donde 0 indica que no existe límite.

Nota: El valor no se verifica.

38-41 Valor que representa el ciclo de vida de un objeto estático, en minutos.

El valor está comprendido entre 0 y 10.080, donde 0 indica que no existe límite.

Nota: El valor no se verifica.

42–45 Valor que representa el intervalo de depuración de la antememoria, en minutos.

El valor está comprendido entre 0 y 720, donde 0 indica que debe inhabilitarse el proceso de recogida de basura.

Subvector de respuesta Depuración: El Subvector de respuesta Depuración se utiliza para responder a un Subvector de respuesta Depuración.

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x0601

6-9 Consulte los “Códigos de retorno” en la página 199.

Subvector de respuesta Consulta: El Subvector de respuesta Consulta se utiliza para comprobar si un URL dado está en la partición de la antememoria.

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x0701

6-9 Código de retorno

Consulte los “Códigos de retorno” en la página 199.

Nota: Si el código de retorno no es correcto (no es 0x00000000), la respuesta terminará aquí.

10-37 Hora en que fue modificado por última vez el objeto, en formato GMT.

Nota: Este campo no existirá si el código de retorno no es 0x00000000 o si no lo conoce la Partición de la antememoria.

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 Estadísticas: El Subvector de respuesta Estadísticas responde al Subvector de mandatos Estadísticas.

0-3 Longitud

Toda la longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x0801

6-9 Código de retorno

Código de retorno del subvector.

10-

10-13 Número actual de bytes de la Partición de la antememoria. Sólo refleja los bytes de entidad y no incluye los bytes utilizados para almacenar los encabezamientos o el control de la utilización de bloques.

14-17 Marca de nivel superior para el número de bytes de la Partición de la antememoria.

18-21 Número actual de objetos en la Partición de la antememoria.

22-25 Marca de nivel superior para el número de objetos de la Partición de la antememoria.

26-29 Número total de veces que se se han encontrado estos objetos en la Partición de la antememoria.

30-33 Número total de veces que no se se han encontrado estos objetos en la Partición de la antememoria.

34-37 Número de objetos que se han añadido a la Partición de la antememoria explícitamente por una máscara de URL de inclusión.

40-43 Número de objetos que no se han añadido a la Partición de la antememoria debido a que se ha desactivado el almacenamiento en antememoria.

44-47 Número de objetos que no se han añadido a la partición de la antememoria debido a que el objeto era demasiado grande.

48-51 Número de objetos que no se han añadido a la Partición de la antememoria debido a que se ha especificado la directiva DONT CACHE en el encabezamiento HTTP de control.

52-55 Número de objetos que no se han añadido a la Partición de la antememoria debido a que se han excluido explícitamente por la máscara de URL.

56-59 Número de objetos que no se han añadido a la Partición de la antememoria debido a que el objeto estaba inactivo.

60-63 Número de objetos que no se han añadido a la Partición de la antememoria debido a que el objeto imagen no se ha almacenado explícitamente en la antememoria.

64-67 Número de objetos que no se han añadido a la Partición de la antememoria debido a que el objeto estático no se ha almacenado explícitamente en la antememoria.

68-71 Número de objetos que no se han añadido a la Partición de la antememoria debido a que el objeto dinámico no se ha almacenado explícitamente en la antememoria.

72-75 Número de objetos depurados a causa de que la antememoria estaba llena o de que todas las particiones de la antememoria superaban la cantidad total permitida por la Antememoria de servidor Web.

76-79 Número de objetos depurados a causa de que el ciclo de vida de los objetos ha finalizado.

80-83 Número de objetos depurados explícitamente, al dar su URL o al depurar toda la partición.

84-87 Número de objetos depurados a causa de la anulación de la dependencia.

Subvector de respuesta Máscara de URL: El Subvector de respuesta Máscara de URL se utiliza para responder a un Subvector de mandatos Máscara de URL.

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave, así como la de los subvectores.

4-5 Clave

0x0901

6-9 Código de retorno

Código de retorno del subvector. Consulte los “Códigos de retorno” en la página 199.

10-n Varios Subvectores URL o ninguno, si el Subvector de mandatos Máscara de URL era Obtener (0x0001).

Formatos de los subcampos

En este apartado se ofrecen las descripciones de los subcampos.

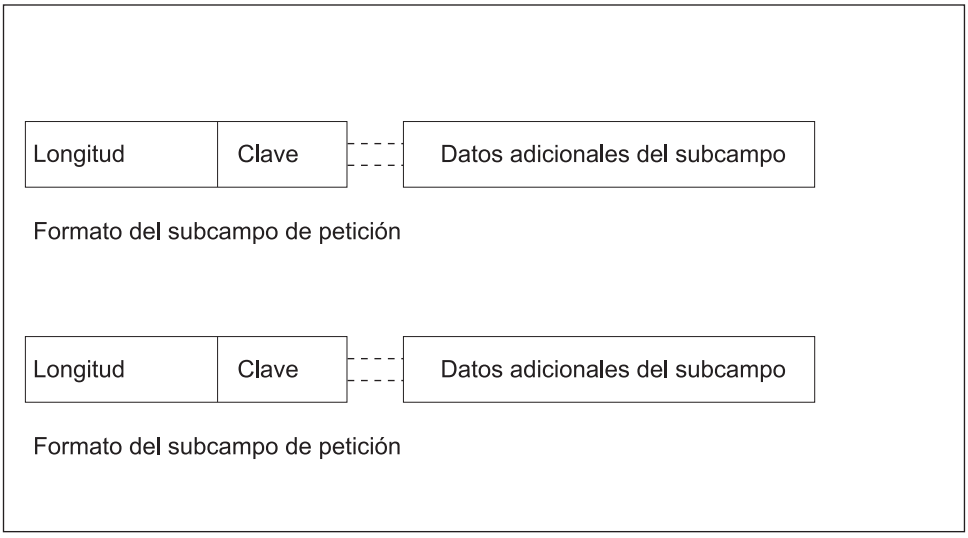


Figura 19. Formato de un subcampo

Longitud: Valor de 32 bits sin signo que representa la longitud (en bytes) de todo el subcampo, incluida la de los campos longitud y clave. Los valores aceptables están comprendidos entre 6 y 4GB.

Clave: Valor de 16 bits sin signo que representa la clave del subcampo. Las claves de los subcampos de mandatos son:

- 0x0010 (Localizador uniforme de recursos, después de desmantelar el protocolo "http:" y la dirección del recurso de Internet. Por ejemplo, el URL "http://192.9.200.50/archivo1.html" se enviaría como "/archivo1.html").
- 0x0020 (Objeto WEB en formato de mensaje de respuesta HTTP)
- 0x0030 (Nombre de usuario del ECCP. El vector de autenticación necesita este subcampo).
- 0x0040 (Contraseña de usuario del ECCP. El vector de autenticación necesita este subcampo).
- 0x0050 (Subcampo Dependencia)

Las claves de los subcampos de respuesta son:

- 0x0011 (Localizador uniforme de recursos, después de desmantelar el protocolo "http:" y la dirección del recurso de Internet).
- 0x0051 (Subcampo Dependencia)

Subcampo Dependencia: El Subcampo Dependencia del Subvector de respuesta Máscara de URL.

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave.

4-5 Clave

0x0050 - petición

0x0051 - respuesta

6-n Dependencia

La longitud debe estar comprendida entre 1 y 50.

Subcampo Nombre: El Subcampo Nombre del Subvector de respuesta Máscara de URL.

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave.

4-5 Clave

0x00030 - petición

6-n Nombre

La longitud debe estar comprendida entre 1 y 8.

Subcampo Objeto: El Subcampo Objeto del Subvector de respuesta Máscara de URL.

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave.

4-5 Clave

0x002 - petición

6-n Objeto

El formato del objeto debe ser el de una Respuesta HTTP. Es una serie de caracteres.

Subcampo Petición de contraseña: El Subcampo Petición de contraseña del Subvector de respuesta Máscara de URL.

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave.

4-5 Clave

0x0400

6-14 El número generador utilizado para el cifrado (deben ser 8 bytes).

15-n Contraseña

La longitud debe estar comprendida entre 1 y 8 bytes y está cifrado.

Subcampo Petición de URL: El Subcampo Petición de URL del Subvector de respuesta Máscara de URL.

0-3 Longitud

Longitud (en bytes) del vector, incluida la de los campos longitud y clave.

4-5 Clave

0x0010 - petición

0x0011 - respuesta

6-n URL o Máscara de URL

Es una serie de caracteres de entre 1 y 255 caracteres.

Códigos de retorno

Es importante comprobar los códigos de retorno de cada subvector de respuesta, además del código de retorno del vector de respuesta. El código de retorno del vector de respuesta se establecerá a un valor distinto de cero en caso de que se detecte un error grave, en cuyo caso, puede que no todos los subvectores de mandatos del vector de mandatos tengan su correspondiente subvector de respuesta.

Códigos de retorno y sus descripciones

0000 0000: La operación se ha realizado satisfactoriamente
0001 0000: No se ha encontrado el objeto
0002 0000: La partición de la antememoria ya está habilitada
0003 0000: La partición de la antememoria ya está inhabilitada
0004 0000: La partición de la antememoria no está habilitada
0005 0000: No se ha definido la partición de la antememoria
0006 0000: La partición de la antememoria está terminando
0007 0000: Es necesario un subcampo URL, pero no está presente
0008 0000: El intervalo de depuración proporcionado no es válido
0009 0000: Valor de configuración 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 los encabezamientos del objeto
0010 0000: Imposible obtener almacenamiento
0011 0000: Objeto demasiado grande para añadirlo a la partición

0012 0000: El formato del vector no es válido
0013 0000: El objeto no puede almacenarse en la antememoria
0014 0000: Detectado error de análisis HTTP
0015 0000: Es necesario un subcampo Objeto, pero no está presente
0016 0000: No se ha proporcionado ningún subcampo Dependencia o no es válido
0017 0000: Es necesario el Vector de autenticación
0018 0000: No es necesario el Vector de autenticación, por lo que se hará caso omiso
0019 0000: La dependencia no estaba en la Tabla de dependencias
001A 0000: El URL de dependencias no estaba en la Tabla de dependencias
001B 0000: Tipo de dependencia no soportado
001C 0000: No es correcto el identificador de usuario, la contraseña o el permiso para el ECC
001D 0000: No es correcto el tipo de máscara de URL para la carga de la imagen en el recuadro
FF01 yyyy: El mandato ha devuelto un error. Los últimos 2 bytes contienen información adicional.
- 0101: No se ha encontrado el objeto.
- 0102: El objeto no se ha podido almacenar en antememoria.
- 0103: El objeto ya existe en la partición.
- 0104: La inicialización de la partición ha dado un error, ya están activas el número máximo de particiones.
- 0105: La partición está activa.
- 0106: La partición no está activa.
- 0107: La partición está en un estado pendiente y no puede ejecutar el mandato. Espere unos segundos y vuelva a intentar ejecutar el mandato.
- 0108: No se ha definido la partición.
- 0109: Tipo de URL no soportado.
- 010A: El puntero de URL no es válido.
- 010B: El número de partición no es válido.
- 010C: Mandato de partición no soportado.
- 010D: El puntero de partición no es válido.
- 010E: El handle de la partición no hace referencia a una partición activa.
- 010F: El handle de la partición no hace referencia a una partición válida.
- 0110: Es necesario un puntero de política, pero no está presente.
- 0111: En necesario un puntero de estadísticas, pero no está presente.
- 0112: El intervalo de depuración es demasiado grande.
- 0113: La dependencia ya tiene URL.
- 0FFF: No está disponible el control de la antememoria externa.
- FFF9: Imposible conseguir espacio de almacenamiento.
- FFFA: Imposible conseguir un handle de partición.
- FFFB: Es necesario un puntero SRAM de política, pero no está presente.
- FFFC: Es necesario un puntero SRAM de partición, pero no está presente.
- FFFD: Imposible asignar o inicializar el intervalo de vencimiento de la antememoria.
- FFFE: Imposible asignar o inicializar la partición de la antememoria.
- FFFF: Imposible asignar o inicializar el núcleo de la antememoria.

Capítulo 12. Configuración y supervisión de la Antememoria de servidor Web

En este capítulo se describe cómo configurar la función Antememoria de servidor Web y cómo utilizar los mandatos de supervisión de la Antememoria de servidor Web. Consta de los apartados siguientes:

- "Configuración de la Antememoria de servidor Web"
- "Acceso al entorno de la Antememoria de servidor Web" en la página 208
- "Mandatos de la Antememoria de servidor Web" en la página 208
- "Acceso al entorno de supervisión de la Antememoria de servidor Web" en la página 215
- "Mandatos de supervisión de la Antememoria de servidor Web" en la página 215.

Configuración de la Antememoria de servidor Web

La función de almacenamiento en Antememoria del servidor Web debe utilizarse con Network Dispatcher. Antes de utilizar la Antememoria de servidor Web por primera vez, deberá:

1. Acceder a Network Dispatcher en el indicador `Config>` de la consola `talk 6` mediante el mandato **feature ndr**.
2. Habilitar el ejecutor
3. Añadir un cluster
4. Añadir un puerto
5. Añadir uno o más servidores.

A continuación podrá utilizar los mandatos de configuración y de supervisión para modificar el entorno de la Antememoria de servidor Web.

Nota: Mientras que los cambios realizados en Network Dispatcher mediante Talk 6 modifican la configuración que se está ejecutando actualmente, los cambios realizados en la Antememoria de servidor Web no modifican la configuración que se está ejecutando actualmente, a menos que se active explícitamente a través del mandato **activate** en Talk 6 o mediante la función Webc de Talk 5. La excepción a esto es que si el cluster o puerto de un Proxy HTTP se elimina mediante la función NDR de Talk 6, también se eliminará de la configuración que se está ejecutando actualmente el proxy HTTP de la Antememoria de servidor Web.

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 ofrece una lista de los parámetros del ejemplo, descritos brevemente.

cluster-address

Especifica la dirección IP del cluster.

Nota: Se supone que las direcciones IP del cluster están en la misma subred lógica que el direccionador de saltos anterior (direccionador IP).

Valores válidos: Cualquier dirección IP

Valor por omisión: 0.0.0.0

FIN-count Especifica el número de conexiones que deben estar en el estado FIN antes de que el ejecutor intente eliminar la información de conexión no usada de la base de datos de Network Dispatcher después de transcurrido el *tiempo de espera de FIN* o el definido en el *temporizador de inactividad*.

Valores válidos: de 0 a 65.535

Valor por omisión: 4.000

FIN-timeout Especifica el número de segundos que una conexión puede permanecer en el estado de FIN antes de que el ejecutor intente eliminar la información de conexión no usada de la base de datos de Network Dispatcher.

Valores válidos: de 0 a 65.535

Valor por omisión: 30

Stale-timer Especifica el número de segundos que una conexión puede permanecer inactiva, después de que el ejecutor intente eliminar la información de la conexión de la base de datos de Network Dispatcher.

Valores válidos: de 0 a 65.535

Valor por omisión: 1500

port# Especifica el número de puerto del protocolo para este cluster.

Valores válidos: de 1 a 65.535

Valor por omisión: 80

port-type Especifica los tipos de tráfico IP cuya carga puede repartirse 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 para los servidores de este puerto. Esto afectara al diferente número de peticiones que el ejecutor entregará a cada servidor.

Valores válidos: de 0 a 100

Valor por omisión: 20

port-mode Especifica si el puerto enviará todas las peticiones de un único cliente a un único servidor (llamado adherente), utilizará ftp pasivo (pftp),utilizará la Antememoria de servidor Web (antememoria), las enviará a un conjunto de antememorias escalables externas (antememoria externa), o no utilizará ningún protocolo concreto para este cluster (ninguno).

Valores válidos: de 0 a 4, donde:

- 0 = none (ninguna)
- 1 = sticky (adherente)
- 2 = pftp

- 3 = cache (antememoria)
- 4 = extcache (antememoria externa)

Valor por omisión: 0

Do you want a new cache partition?
Especifica si quiere utilizar una partición de la antememoria ya existente o una nueva.

Valores válidos: Yes (Sí) o No

Valor por omisión: Yes (Sí)

Enter cache partition
Especifica el número de la partición de la antememoria ya existente que se utilizará.

Valores válidos: Cualquier número de partición de la antememoria ya existente

Valor por omisión: 0

Default server TCP connection timeout
Especifica el tiempo que transcurrirá antes de que finalice la conexión con un servidor.

Valores válidos: de 5 a 240 segundos

Valor por omisión: 120 segundos.

Do you want to modify cache partition?
Le permite modificar la configuración de una partición de la antememoria ya existente.

Valores válidos: Yes (Sí) o No

Valor por omisión: No

Default client TCP connection timeout
Especifica el tiempo que transcurrirá antes de que finalice la conexión con un cliente.

Valores válidos: de 5 a 240 segundos

Valor por omisión: 120 segundos.

Maximum partition size
Especifica la cantidad máxima de memoria que se asignará a esta partición de la antememoria. Si este valor es superior a la cantidad de memoria disponible actualmente, se hará caso omiso del valor y no se impondrá ningún tamaño máximo de la partición.

Valores válidos: de 1 a 4095 Megabytes o 0 (sin máximo)

Valor por omisión: 0 (sin máximo)

Maximum number of objects
Especifica el número máximo de objetos que pueden almacenarse en una partición de la antememoria. Si el usuario escribe un 0, la partición de la antememoria estará limitada solamente por la cantidad de memoria disponible para la partición.

Valores válidos: de 1 a 100.000 ó 0 (sin límite)

Valor por omisión: 0 (sin límite)

Maximum object size

Especifica el tamaño máximo de los objetos que se almacenarán en la antememoria. Loa objetos que superen este tamaño máximo nunca se almacenarán en la antememoria. Si se modifica el tamaño máximo de los objetos después de llenar la antememoria, es posible que algunos objetos que ya estaban en la antememoria tengan temporalmente un tamaño superior al máximo que se ha definido.

Valores válidos: de 512 a 300.000 bytes o 0 (sin tamaño máximo)

Valor por omisión: 0 (sin tamaño máximo)

Do you want the cache activated upon reboot?

Especifica si una partición de la antememoria debe activarse automáticamente o sólo cuando lo solicite explícitamente el usuario. Las particiones de la antememoria configuradas para que se activen inmediatamente se habilitan automáticamente al rearrancar el 2212. Las particiones de la antememoria que no están configuradas para activarse inmediatamente permanecerán inhabilitadas hasta que el usuario active la partición desde la consola `talk 5` de la Antememoria de servidor Web.

Valores válidos: Yes (Sí) o No

Valor por omisión: Yes (Sí)

Default cache purge interval

Especifica el intervalo de depuración por omisión de la antememoria.

Valores válidos: de 1 a 720 minutos o 0 (inhabilitado)

Valor por omisión: 10 minutos

Enable transparent caching?

Especifica si las respuestas del servidor a objetos que no se han encontrado (no encontrados en la antememoria) deben almacenarse automáticamente en la antememoria.

Valores válidos: Yes (Sí) o No

Valor por omisión: Yes (Sí)

Check cache control headers?

Permite que un servidor especifique a la Antememoria de servidor Web si la respuesta se puede elegir para ser almacenada en antememoria.

Valores válidos: Habilitado o Inhabilitado

Valor por omisión: Inhabilitado

Cache images?

Especifica si los archivos de imágenes (*.gif o *.jpg) deben almacenarse en antememoria.

Valores válidos: Yes (Sí) o No

Valor por omisión: Yes (Sí)

Default expiration time for images

Valores válidos: de 1 a 10.080 minutos, o 0 (ninguna)

Valor por omisión: 60 minutos

Cache non-image static objects?

Especifica si datos estáticos que no son imágenes (archivos que no contenga la máscara */cgi* y archivos que no terminen en .jpg o .gif) deben almacenarse en antememoria.

Valores válidos: Yes (Sí) o No

Valor por omisión: Yes (Sí)

Default expiration time for non-image static objects

Valores válidos: de 1 a 10.080 minutos, o 0 (ninguna)

Valor por omisión: 60 minutos

URL mask to identify dynamic objects

Especifica la máscara de URL que se utilizará para identificar objetos dinámicos.

Valores válidos: cualquier máscara de URL

Valor por omisión: */cgi*

Cache dynamic objects?

Especifica si deben almacenarse en la antememoria los objetos dinámicos. Los objetos dinámicos son objetos que construye el servidor al recibir la petición del objeto y que reconstruye a cada nueva petición, hayan cambiado o no los datos.

Valores válidos: Yes (Sí) o No

Valor por omisión: No

Do you want to add a URL mask?

Especifica una máscara de URL nueva que se añadirá a la antememoria. Las máscaras de URL permiten que el usuario incluya o excluya objetos individuales o grupos de objetos por su Localizador universal de recursos (URL).

Valores válidos: i o e

Valor por omisión: i

Cuando se especifica una máscara de URL, se pueden utilizar caracteres comodín. Al configurar Network Dispatcher para la Antememoria del servidor Web o al utilizar los mandatos **add** o **modify url** desde el indicador `f webc`, pueden utilizarse caracteres comodín. Los caracteres utilizados como comodines son el * (asterisco) y el # (signo de número). Los comodines pueden utilizarse en cualquier posición del URL.

El signo * indica que o ningún carácter o cualquier número de caracteres forman parte del URL:

Ejemplo: *abc.html filtrará las máscaras de URL siguientes.

```
abc.html
finabc.html
defchtjqsprabc.html
```

El signo # representa un solo carácter.

Ejemplo: ab#.html filtrará las máscaras de URL siguientes.

```
abc.html
abf.html
abo.html
```

En el ejemplo siguiente se selecciona la modalidad de puerto 3 (cache=3) y no se añade ninguna partición de la antememoria nueva.

```
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: En el ejemplo siguiente se selecciona la modalidad de puerto 3 (cache=3) y se añade una partición de la antememoria nueva.

```
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>
```

Para configurar el cluster y el puerto iniciales para la función de almacenamiento en la Antememoria del servidor Web, debe utilizarse Network Dispatcher. Una vez añadidos el cluster y el puerto, al configurar la *modalidad de puerto* como puerto de

la antememoria, podrá modificar y visualizar los parámetros de configuración del almacenamiento en Antememoria del servidor Web en el indicador WEBC Config>.

Consulte la página 126 para obtener más información sobre Network Dispatcher.

Acceso al entorno de la Antememoria de servidor Web

Para acceder al entorno de configuración de la Antememoria de servidor Web, escriba el mandato siguiente en el indicador Config>.

```
Config> feature webc
WEBC Config>
```

Mandatos de la Antememoria de servidor Web

En este apartado se describen los mandatos de configuración de la Antememoria de servidor Web. En la Tabla 18 se listan los mandatos de configuración de la Antememoria de servidor Web. Estos mandatos especifican los parámetros de la función Antememoria de servidor Web. Para activar los cambios, reinicie el direccionador.

Tabla 18. Resumen de mandatos de configuración de la Antememoria de servidor Web

Mandato	Función
? (Ayuda)	Visualiza todos los mandatos disponibles para este nivel de mandato, o lista las opciones de mandatos específicos (si es que están disponibles). Consulte "Obtención de ayuda" en la página xxv.
Activate	Activa las particiones de la 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 del almacenamiento en antememoria.
Modify	Modifica la información del almacenamiento en antememoria.
Exit	Hace volver al nivel de mandato anterior. Consulte "Salida de un entorno de nivel inferior" en la página xxv.

Activate

Utilice el mandato **activate** para inicializar todas las particiones de la antememoria, utilizando la configuración más reciente.

Sintaxis:

ac**tivate**

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 **d** urlmask

Ejemplo:

```
WEBC Config>add url
Partition number [0]?
New URL mask []? *mascaranueva*
Include or Exclude from cache (i or e) [i]? i
Set default expiration time?  [No]:y
Default expiration time
        (1-10080 minutes or 0 for no expiration) [0]? 20
The URL mask has been added to cache partition number 0.
```

Nota: Para añadir proxies y particiones, deberá utilizar Network Dispatcher y ejecutar los mandatos **add port** o **set port**.

partition number
Número de partición que se añadirá a la partición.

Valores válidos: cualquier número de partición válido

Valor por omisión: 0

new URL mask
Nombre de la máscara de URL que se añadirá.

Valores válidos: Cualquier máscara de URL válida

Valor por omisión: ninguno

include or exclude from cache
Especifica si el URL debe incluirse en la antememoria o excluirse de ella.

Valores válidos: i o e

Valor por omisión: i

default expiration time
Especifica la hora de vencimiento por omisión, en minutos. Un cero indica que no tiene hora de vencimiento.

Valores válidos: de 0 a 10.080 minutos

Valor por omisión: 0 (sin hora de vencimiento)

Delete

Utilice el mandato **delete** para suprimir una máscara de URL o una partición.

Sintaxis:

de **lete** partition
urlmask

partition
Número de la partición que se suprimirá de una antememoria.

urlmask
Nombre de la máscara de URL que se suprimirá 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 deberá utilizar la función realizar una conversión "proxy" y eliminar el puerto y el cluster asociados, o cambiar la modalidad de puerto a otra distinta de la de antememoria.

partition number
Número de partición que se suprimirá de la partición.

Valores válidos: cualquier partición válida

Valor por omisión: 0

URL mask number
Número de la máscara de URL que se suprimirá.

Valores válidos: cualquier número de máscara de URL válido.

Valor por omisión: 1

List

Utilice el mandato **list** para listar la información de la Antememoria de servidor Web.

Sintaxis:

list all
external
partition
proxy
urlmask

all List todos los puertos, particiones, proxies y máscaras definidos en una antememoria.

external
Lista la información del Gestor de control de la antememoria externa.

partition
Lista los números de partición de una antememoria.

proxy Lista los proxies definidos en una antememoria.

urlmask
Lista las máscaras de URL 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 de la Antememoria del servidor Web.

Sintaxis:

modify external
partition
proxy
urlmask

external
Le permite modificar el Gestor de control de la antememoria externa.

partition
Le permite modificar una partición.

proxy Le permite modificar el proxy

urlmask
Le 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
Especifica el número de puerto del gestor de control de la antememoria externa que se va a modificar.

Valores válidos: de 0 a 255

Valor por omisión: 82

TCP connection timeout
Especifica la conexión TCP del gestor de control de la antememoria externa que se va a modificar.

Valores válidos: de 5 a 240 segundos

Valor por omisión: 120

do you want to modify the encryption key
Especifica si se ha de modificar o no la clave de cifrado.

Valores válidos: yes (sí) o no

Valor por omisión: no

encryption key
Clave de cifrado para el gestor de control de la antememoria externa que se va a modificar. La clave de cifrado debe ser una serie de 16 caracteres hexadecimales.

Valores válidos: caracteres 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 la partición que se modificará.

Valores válidos: cualquier número de partición válido

Valor por omisión: 0

maximum partition size
Tamaño máximo de la partición que se modificará. Un cero indica que no existe límite.

Valores válidos: de 1 a 255 megabytes o 0 para indicar que no existe límite

Valor por omisión: 0

maximum number of objects
Número máximo de objetos en la partición que se modificará. Un cero indica que no existe límite.

Valores válidos: de 0 a 100.000 ó 0 para indicar que no hay límite

Valor por omisión: 0

maximum object size
Tamaño máximo de los objetos de la partición que se va a modificar. Un cero indica que no existe límite.

Valores válidos: de 512 a 300.000 ó 0 para indicar que no hay límite

Valor por omisión: 0

do you want the cache activated upon reboot
Especifica si se ha de activar o no la antememoria después de rearrancar.

Valores válidos: yes (sí) o no

Valor por omisión: yes (sí)

default cache purge interval
Especifica el intervalo de depuración por omisión de la antememoria. Un cero inhabilita el intervalo de depuración por omisión de la antememoria.

Valores válidos: de 1 a 170 minutos o 0 para inhabilitarlo

Valor por omisión: 10

enable transparent caching
Especifica si se ha de habilitar o no el almacenamiento transparente en antememoria.

Valores válidos: yes (sí) o no

Valor por omisión: yes (sí)

check cache control headers
Especifica si se han de comprobar o no los encabezamientos de control de la antememoria.

Valores válidos: yes (sí) o no

Valor por omisión: yes (sí)

cache images
Especifica si se han de almacenar las imágenes en antememoria.

Valores válidos: yes (sí) o no

Valor por omisión: yes (sí)

Default expiration time for images
Especifica la hora de vencimiento por omisión de las imágenes. Un cero indica que no existe hora de vencimiento.

Valores válidos: de 1 a 10.080, ó 0 para indicar que no existe hora de vencimiento.

Valor por omisión: 60

cache non-image static objects
Especifica si se han de almacenar en antememoria los objetos estáticos que no son imágenes.

Valor por omisión: yes (sí)

Valores válidos: yes (sí) o no

Default expiration time for non-image static objects
Especifica la hora de vencimiento por omisión de los objetos estáticos que no son imágenes. Un cero indica que no existe hora de vencimiento.

Valores válidos: de 1 a 10.080, ó 0 para indicar que no existe hora de vencimiento.

Valor por omisión: 60

url mask to identify dynamic objects
Especifica la máscara de URL que se utilizará para identificar objetos dinámicos.

Valores válidos: cualquier máscara de url válida

Valor por omisión: */cgi*

cache dynamic objects
Especifica si se han de almacenar en antememoria los objetos dinámicos.

Valores válidos: yes (sí) 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
Especifica el número de partición del URL que se va a modificar.

Valores válidos: cualquier número de partición válido

Valor por omisión: 0

url mask number
Especifica el número de la máscara de URL que se va a modificar.

Valores válidos: cualquier número de máscara de URL válido.

Valor por omisión: 1

new url mask *stat*

Valores válidos: yes (sí) o no

Valor por omisión: yes (sí)

include or exclude from cache
Especifica si incluir o no, o excluir o no el URL modificado en la antememoria.

Valores válidos: i o e

Valor por omisión: i

set default expiration time
Especifica si se ha de establecer o no la hora de vencimiento por omisión.

Valores válidos: yes (sí) o no

Valor por omisión: yes (sí)

default expiration time
Especifica la hora de vencimiento por omisión, en minutos. Un cero indica que no hay hora de vencimiento.

Valores válidos: de 1 a 10.080 minutos, ó 0 para indicar que no hay hora de vencimiento.

Valor por omisión: 0

Acceso al entorno de supervisión de la Antememoria de servidor Web

Para acceder al entorno de supervisión de la Antememoria de servidor Web, escriba el mandato **f webc** en el indicador de configuración `t 5`.

```
t 5>f webc
```

Mandatos de supervisión de la Antememoria de servidor Web

La Tabla 19 lista los mandatos de supervisión de la Antememoria de servidor Web.

Tabla 19 (Página 1 de 2). Resumen de los mandatos de supervisión de la Antememoria de servidor Web

Mandato	Función
? (Ayuda)	Visualiza todos los mandatos disponibles para este nivel de mandato, o lista las opciones de mandatos específicos (si es que están disponibles). Consulte “Obtención de ayuda” en la página xxv.
Activate	Activa las particiones de la antememoria utilizando la configuración más reciente.
Clear	Borrar una partición o las estadísticas de una partición.

Tabla 19 (Página 2 de 2). Resumen de los mandatos de supervisión de la Antememoria de servidor Web

Mandato	Función
Enable	Habilita una partición.
Delete	Suprime una partición, proxy o máscara de URL.
Disable	Inhabilita una partición.
List	Lista la información del almacenamiento en antememoria.
Modify	Modifica la información del almacenamiento en antememoria.
Exit	Hace volver al nivel de mandato anterior. Consulte “Salida de un entorno de nivel inferior” en la página xxv.

Activate

Utilice el mandato **activate** para activar todas las Antememorias del servidor Web o una partición o proxy determinados.

Sintaxis:

ac**tivate** all
ex**t**ernal
pa**r**tition
pr**o**xy

all Activa todas las antememorias definidas.

external
Activa el Gestor de control de la 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 las estadísticas de una partición.

Nota: Al borrar los objetos de la partición, no se borran 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
Especifica el número de partición que se va a 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 la partición que se va a habilitar.

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:

```
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
Especifica el número de la partición que se va a 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
Especifica el número de la partición que se va a inhabilitar.

Valores válidos: cualquier número de partición válido

Valor por omisión: 0

List

Utilice el mandato **list** para visualizar la información de todos los almacenamientos de Antememorias del servidor Web, de una partición, de una política o de un proxy.

Sintaxis:

list all
delete
depend
external
item
partition
policy
proxy

all Lista todas las particiones, políticas y proxies de una antememoria.

delete Lista los 100 últimos elementos suprimidos de la partición de la antememoria.

depend
Lista la tabla de dependencias de la partición.

external
Lista la información del Gestor de control de la antememoria externa.

item Lista los elementos y el contador de aciertos actuales de la partición de la antememoria.

partition
Lista la información sobre una partición de la antememoria.

policy Lista la información sobre las políticas de la antememoria.

proxy Lista la información sobre un proxy de 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
'/futbol.html' -- 2
'/tenis.html' -- 1
'/curling.html' -- 3
```

Ejemplo:

```
WEBC>list depend
Enter partition number: [0]?

Dependency table for Partition 0
--------------------------------------
dep: tenis_info
   count of URLs: 2
   URLs:
         tenis_schedule.html
         tenis_roster.html
dep: futbol_info
   count of URLs: 2
   URLs:
         futbol_schedule.html
         futbol_roster.html
dep: roster
   count of URLs: 2
   URLs:
         futbol_roster.html
         tenis_roster.html
dep: schedule
   count of URLs: 2
   URLs:
         futbol_schedule.html
         tenis_schedule.html
```

Ejemplo:

```
WEBC>list item
Enter partition number: [0]? 0
Current number of items: 5
URL String -- hit count
======================
'/' -- 2
'/archiv5k.html' -- 1
'/archiv4k.html' -- 1
'/archiv2k.html' -- 3
'/archiv1k.html' -- 1
```

Ejemplo:

```
WEBC>li 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>li pol
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: Proxy que forma parte del conjunto de antememorias.

```
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: Proxy que no forma parte del conjunto de antememorias.

```
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 la antememoria externa.

Sintaxis:

m**odify** 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

TCP connection timeout

do you want to modify the encryption key

encryption key

Configuración y supervisión de la Antememoria de servidor Web

Capítulo 13. Configuración y supervisión del subsistema de codificación

Las funciones de compresión de y de cifrado de datos se agrupan en el Subsistema de codificación (ES, Encoding Subsystem). El Subsistema de codificación permite que las interfaces o protocolos accedan a los dispositivos de codificación y se activa automáticamente al activar un enlace de compresión o cifrado. En la plataforma 2212, los dispositivos de codificación son el Adaptador de compresión y cifrado (CEA, Compression/Encryption Adapter) y el dispositivo software. El dispositivo software consiste en un software operativo que realiza la compresión y el cifrado. Cuando se utiliza el dispositivo software, los algoritmos de compresión y cifrado se ejecutan en el procesador del direccionador. No es necesario cambiar la configuración por omisión para utilizar el CEA o el dispositivo software.

Puede supervisarse la actividad del ES escribiendo **feature es** desde el indicador de supervisión (talk 5).

Los parámetros de configuración del ES permiten limitar la cantidad de memoria que utilizará el dispositivo software del ES. La configuración por omisión permite que el ES disponga de tanta memoria como necesite. Para limitar el uso de la memoria, ejecute el mandato **set**, después de **feature es**, en el proceso de configuración (talk 6).

Este capítulo consta de los apartados siguientes:

- "Configuración del subsistema de codificación"
- "Supervisión del subsistema de codificación" en la página 225

Configuración del subsistema de codificación

Los parámetros de configuración del ES permiten controlar el número de sesiones de compresión y cifrado que podrá manejar simultaneamente el dispositivo software de codificación. El dispositivo software de codificación consiste esencialmente en una colección de bibliotecas de compresión y cifrado que se ejecutan en el procesador del direccionador. Una sesión consiste en una conexión dúplex a través de una interfaz determinada configurada para que utilice las funciones de compresión o de cifrado.

Nota: Los parámetros de configuración del ES influyen solamente sobre el dispositivo software de codificación, no sobre el CEA.

En general, la codificación de datos es una operación que consume muchos recursos del procesador. Al limitar el número de sesiones de codificación, se puede controlar hasta cierto punto el impacto de la codificación de datos en el rendimiento del direccionador. Por ejemplo, si el direccionador tiene 20 interfaces de marcación configuradas para que utilicen la función de compresión y se ha determinado que comprimir con más de 10 interfaces a la vez produce un efecto negativo en el rendimiento del direccionador, debe establecerse que el número máximo de sesiones de compresión es de 10. Esto permite que 10 de las 20 interfaces utilicen la función de compresión.

Las necesidades de memoria del dispositivo software de codificación también son una razón para limitar el número de sesiones. Cada sesión de compresión utiliza aproximadamente 30 KB de la memoria del direccionador y una sesión de cifrado

utiliza aproximadamente 2 KB. Si el ES utiliza demasiada memoria, otras funciones podrán sufrir restricciones de memoria y el rendimiento del direccionador se verá afectado negativamente. Consulte el apartado “Consideraciones” en la página 234 para obtener más información.

Se puede establecer el número mínimo o máximo de sesiones del ES haciendo constar el número de sesiones o especificando un número o uno de los valores *unlimited (ilimitado)*, *default (por omisión)*. Los valores *unlimited* y *default* tienen el mismo significado: ambos permiten que el direccionador dé soporte a todas las sesiones que se activen para cifrado o compresión, mientras no se agote la memoria.

Nota: Ninguno de los parámetros de configuración del ES (talk 6) pueden reconfigurarse dinámicamente. Para activar los valores de los parámetros después de cambiarlos, deberá reiniciar o volver a cargar el direccionador.

En el proceso de Configuración (talk 6), escriba **feature es** en el indicador `Config>` para acceder a los mandatos de configuración del ES. Aparecerá el indicador `ES Config>`. En la Tabla 20 se listan los mandatos.

Tabla 20. Mantados de configuración del ES

Mandato	Acción
? (Ayuda)	Visualiza todos los mandatos disponibles para este nivel de mandato, o lista las opciones de mandatos específicos (si es que están disponibles). Consulte “Obtención de ayuda” en la página xxv.
List	Muestra la configuración actual de las sesiones de compresión y cifrado.
Set	Establece el número máximo de sesiones de cifrado y compresión disponibles para todas las interfaces.
Exit	Hace volver al nivel de mandato anterior. Consulte “Salida de un entorno de nivel inferior” en la página xxv.

List

Utilice el mandato **list** para visualizar la configuración 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 establecer el número máximo de sesiones de cifrado y 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 una abreviatura de software.

software minimum compression-sessions *n, unlimited o default*
Establece el número mínimo de sesiones de compresión disponibles para las interfaces. El direccionador reserva este número de sesiones de forma que siempre estarán disponibles.

Valor por omisión: 0

Valores válidos: de 0 a *unlimited*; alternativamente, *default*

software maximum compression-sessions *n, unlimited o default*
Establece el número máximo de sesiones de compresión disponibles para las interfaces. Una vez se activa este número, no se podrán activar más sesiones.

Valor por omisión: 0

Valores válidos: de 0 a *unlimited*; alternativamente, *default*

software minimum encryption-sessions *n, unlimited o default*
Establece el número mínimo de sesiones de cifrado disponibles para las interfaces. El direccionador reserva este número de sesiones de forma que siempre estarán disponibles.

Valor por omisión: 0

Valores válidos: de 0 a *unlimited*; alternativamente, *default*

software maximum encryption-sessions *n, unlimited o default*
Establece el número máximo de sesiones de cifrado disponibles para las interfaces. Una vez se activa este número, no se podrán activar más sesiones.

Valor por omisión: 0

Valores válidos: de 0 a *unlimited*; alternativamente, *default*

Supervisión del subsistema de codificación

En el proceso de supervisión, escriba **feature es** en el indicador `+` para acceder a los mandatos de supervisión del ES. Aparecerá el indicador `ES Monitor>`. En la Tabla 21 en la página 226 se listan los mandatos disponibles.

Tabla 21. Mandato de supervisión del ES

Mandato	Acción
? (Ayuda)	Visualiza todos los mandatos disponibles para este nivel de mandato, o lista las opciones de mandatos específicos (si es que están disponibles). Consulte “Obtención de ayuda” en la página xxv.
List	Muestra información detallada sobre los puertos, los circuitos, los dispositivos, la configuración y el estado del ES, o muestra un resumen.
Exit	Hace volver al nivel de mandato anterior. Consulte “Salida de un entorno de nivel inferior” en la página xxv.

List

Utilice el mandato **list** para mostrar información sobre el ES. En el apartado en el que se describe el mandato **list summary**, se da un ejemplo de la salida del mandato **list**, en que aparece información sobre los puertos, lso dispositivos y el estado del ES.

Sintaxis:

list ports
circuits
devices
config
status
summary

ports El mandato **list ports** lista los puertos de codificación creados por los clientes potenciales del sistema de codificación. Un puerto establece un enlace entre el sistema de codificación y los clientes configurados para utilizar el ES. Por ejemplo, si las funciones de compresión o cifrado están configuradas a través de la interfaz Net 1 PPP, se asociará un puerto con dicha interfaz. El campo QLen muestra la suma de todas las peticiones de compresión o de cifrado pendientes para todos los circuitos asociados con el puerto. Un cliente, como por ejemplo el protocolo PPP configurado para una interfaz determinada, presenta una petición al ES cuando asigna para codificación un almacenamiento intermedio de datos concreto.

El campo Status muestra *Idle (Desocupado)* si no hay ningún petición en la cola del puerto o *Busy (Ocupado)* o *Waiting (En espera)*, si las peticiones se están procesando o están en la cola del puerto.

circuits

El mandato **list circuits** muestra los circuitos definidos por los clientes del sistema de codificación. Cada circuito corresponde a una conexión dúplex. Los datos cifrados o comprimidos en un extremo se descifran o descomprimen en el otro.

Por omisión, sólo se mostrarán los circuitos activos. Utilice el mandato **list circuits all** para incluir los circuitos activos e inactivos.

Para cada circuito encontrado, se mostrarán el puerto y el usuario, igual que en el mandato **list ports**. Además, se mostrarán dos líneas de información; una línea Tx para el circuito de salida y una línea Rx para el circuito de entrada. El identificador del circuito es un número arbitrario suministrado por el cliente, para que pueda identificar todos los circuitos que cree. Para los circuitos Frame Relay, este número corresponde al

identificador del circuito Frame Relay de enlace de datos (DLCI) asociado. Los enlaces Punto a punto sólo crean un circuito, identificado siempre por el número *1*.

Además, también se muestran los siguientes puntos:

Dev Número que representa el dispositivo de codificación que atiende esa corriente. Es 1 cuando la codificación la realiza el software utilizando la CPU y 2 cuando la codificación la realiza el adaptador de compresión y cifrado.

Cmpr Campo que muestra el algoritmo de compresión o descompresión que está activo para esta corriente. Si es *LZC*, significa que se está utilizando el método de compresión STAC-LZC; si es *MPPC*, se está utilizando el método PPC, de Microsoft®. Se añadirá un asterisco (*) al nombre del algoritmo, si la corriente opera en modalidad sin información de estado. La modalidad sin información de estado es una modalidad en la que no se mantiene la historia de los paquetes de datos después de procesarlos, al contrario de lo que ocurre en la modalidad continua, en la que se mantiene la historia de cada paquete que se ha manejado para poder manejar el siguiente. Por ejemplo, en la modalidad de compresión continua, el codificador mantiene almacenada en una antememoria información sobre los paquetes anteriores, con el fin de poder comprimir los paquetes actuales.

Encr Campo que muestra el algoritmo de cifrado o descifrado que se está utilizando. Es *DES* para el algoritmo DES estándar, *3DES* para el algoritmo Triple DES o *RC4* si se utiliza el algoritmo RC4, de RSA'. Se añadirá un asterisco (*) al nombre del algoritmo, si el stream is operating en modalidad sin información de estado. Esto tiene importancia en el algoritmo RC4, pero apenas significa nada para los algoritmos DES/3DES. Obsérvese que el nombre que aparece corresponde al algorítmo de cifrado básico utilizado, no al formato de encapsulación utilizado por el cliente. Por ejemplo, el protocolo PPP da soporte a dos métodos de encapsulación: DESE (RFC 1969) que utiliza el algoritmo de cifrado DES, y MPPE (método no estándar de Microsoft), que utiliza el RC4.

QLen Este parámetro muestra el número de paquetes de salida que esperan en la cola de la corriente a ser codificados o decodificados. Obsérvese que este número sólo muestra los paquetes que realmente se han enviado al ES para ser procesados. Algunos clientes pueden poseer sus propias colas y, desde ellas, enviar al sistema de codificación sólo unos pocos paquetes cada vez.

Status Una rápida ojeada al estado de las corrientes. No es extraño ver que todas las corrientes estén en espera y que ninguna esté ocupada. Ver alguna corriente en estado ocupado significaría haber atrapado la actividad de la cola durante una ventana de tiempo muy pequeña del ciclo de proceso. Los estados posibles son:

Idle No hay paquetes en la cola de esta corriente

Busy En este momento, el sistema está procesando paquetes de esta corriente (lo que quiere decir que el elemento en cabeza de la cola está siendo procesado por el motor de codificación en este momento).

Waiting
Las peticiones están pendientes, pero actualmente no se está procesando ninguna de esa corriente.

devices

El mandato **list devices** lista los dispositivos de codificación que el sistema tiene disponibles. Un dispositivo de codificación generalmente se refiere a un adaptador de compresión y cifrado. El software que se utiliza cuando no se disponde de un acelerador hardware, está implementado como dispositivo virtual y también aparecerá en está lista como dispositivo *Host Software (Software del sistema principal)*. Este mandato tiene dos formas: **list devices** y **list device n**. La primera genera un listado que es un resumen breve de todos los dispositivos reconocidos por el sistema. La segunda genera un listado detallado de un determinado dispositivo n, donde n es el número de la unidad. La unidad 1 representa el software del sistema principal, que es un dispositivo de codificación virtual, y la unidad 2 representa el adaptador de compresión y cifrado. Puede utilizarse un asterisco (*) en lugar del número n, en cuyo caso, se generará un listado para ambas unidades.

config El mandato **list config** muestra los parámetros actuales de configuración. Estos son los parámetros que se leen de la memoria no volátil cuando el direccionador se reinicia o se vuelve a cargar. La información que se muestra es idéntica a la que se muestra por el mandato de configuración (talk 6) **list config**.

status El mandato **list status** muestra el estado del sistema de codificación, y consiste en varios distintivos globales de estado y en varias estadísticas sobre el sistema. Estas son las descripciones de los campos que se muestran con el mandato **list status**:

Last Error

Último código de error devuelto a los clientes del sistema de codificación. Sirve con propósitos de depuración y debe utilizarse solamente por personal del servicio técnico.

Internal Condition flags

Este campo muestra determinadas condiciones internas, definidas en la lista siguiente:

Ready El sistema está en funcionamiento y es operativo. Esta es la condición normal.

Not Working

El sistema de codificación no está operativo a causa de un error interno.

No Devices Available

Indica que no hay dispositivos disponibles para realizar la codificación. Esta condición no debería producirse, ya que si no existe un codificador hardware, la codificación la llevará a cabo software interno.

Out of Memory

El sistema ha intentado asignar memoria y no ha podido. Esta condición indica que el direccionador se está quedando sin memoria RAM y que el sistema de codificación se está viendo afectado negativamente.

Number of Ports

Campo que indica el número de clientes que ha establecido por su cuenta algún puerto en el ES. En el mandato **list ports** se ofrece la definición de puerto.

Number of Circuits

En el mandato **list circuits** se ofrece una definición de circuito.

Global Request pool size
Número de almacenamientos intermedios de peticiones asignados y libres. Se utiliza aproximadamente un almacenamiento intermedio de peticiones por cada paquete codificado. Si el número de almacenamientos intermedios libres es menor que el número de asignados, significa que el proceso de codificación está en marcha.

Total # of Requests processed
Valor que muestra el número total de almacenamientos intermedios procesados por el motor de codificación. Este número se corresponde aproximandamente con el número total de paquetes comprimidos y cifrados por todos los clientes del sistema desde la última vez que se reinició o se volvió a cargar el direccionador.

summary
Este mandato muestra 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
------ --------------------------  ---------  ----------
     2 Hardware Accelerator/0        2/1     Ready
     1 Host Software                 0/0     Ready
     0 Null Device                   0/0     Ready


                        Encoding System Ports
                        ---------------------

                                 +--Encoder State---+   +--Decoder State---+
Port  User                       QLen  Status           QLen  Status
----  -------------------------  ----  --------------   ----  --------------
   1  Net 2   (PPP/0)               0  Idle                0  Idle
   2  Net 3   (PPP/1)               0  Idle                0  Idle
```

Capítulo 14. Configuración y supervisión de la compresión de datos

En este capítulo se trata de la compresión de datos en un 2212 sobre las interfaces Frame Relay y PPP. Consta de los apartados siguientes:

- "Visión general de la compresión de datos"
- "Conceptos de la compresión de datos"
- "Configuración y supervisión de la compresión de datos para enlaces PPP" en la página 236
- "Configuración y supervisión de la compresión de datos para enlaces Frame Relay" en la página 239

La compresión de datos está soportada para las interfaces Frame Relay y PPP.

Visión general de la compresión de datos

El sistema de compresión de datos proporciona un medio de aumentar el ancho de banda efectivo de las interfaces de red del dispositivo. Está pensado para utilizarlo principalmente en enlaces WAN de baja velocidad.

La compresión de datos en el dispositivo está soportada para las interfaces PPP y Frame Relay:

- Para interfaces PPP, la compresión está implementada según el Protocolo de control de compresión (CCP), definido en el documento RFC 1962 del Comité de Ingeniería de Internet. El CCP proporciona los mecanismos básicos utilizados para la negociación del uso de la compresión y un medio para elegir entre varios protocolos de compresión.

  El dispositivo proporciona dos protocolos de compresión: el protocolo Stac-LZS, definido en el documento RFC 1974; y el protocolo de Compresión punto a punto de Microsoft (MPPC), descrito en el documento RFC 2118. Ambos están basados en algoritmos de compresión de Stac Electronics.
- Para interfaces Frame Relay, la compresión está implementada según el FRF.9, el *Acuerdo de implementación de compresión de datos a través de Frame Relay* desarrollado por el Comité técnico del foro de debate sobre Frame Relay. El FRF.9 describe un Protocolo de compresión de datos (DCP), modelado a partir del CCP de la interfaz PPP y, de forma similar, proporciona un medio para negociar varios algoritmos y opciones de compresión. El dispositivo soporta la "modalidad 1" de negociación del DCP. El FRF.9 también describe una "modalidad 2" más general, pero no está soportada. La propia compresión se realiza mediante el mismo motor de compresión que se utiliza para el protocolo Stac-LZS de la interfaz PPP.

Conceptos de la compresión de datos

La compresión de datos en el dispositivo proporciona un medio de aumentar el rendimiento de los enlaces de una red, al hacer un uso más eficiente del ancho de banda disponible para un enlace. El principio básico subyacente esto es sencillo: representar el flujo de datos que atraviesa un enlace de forma tan compacta como sea posible, de manera que el tiempo necesario para transmitirlo sea el menor posible, dada una velocidad establecida para el enlace.

La compresión de datos puede realizarse en varias capas del modelo de red. En un extremo, las aplicaciones pueden comprimir los datos antes de transmitirlos a sus iguales en cualquier lugar de la red, mientras que en el otro extremo, los dispositivos pueden realizar la compresión en la capa de enlace de datos, trabajando únicamente con la corriente de bits que pasa entre dos nodos. La forma en que se realiza la compresión y su eficacia depende de muchos factores, como por ejemplo en qué capa de red se realiza la compresión, cuál es el conocimiento intrínseco que tienen el compresor y el descompresor de los datos que van a comprimirse, el algoritmo de compresión que se ha escogido o el tipo de datos a comprimir. Normalmente, la mejor compresión la consigue la capa de aplicación; por ejemplo, una aplicación de transmisión de archivos puede permitirse el lujo de disponer de todo el archivo de datos antes de realizar la compresión, y puede poder probar varios algoritmos de compresión para ver con cuál se logra una mejor compresión de los datos de ese archivo en particular. Aunque así se puede conseguir una compresión excelente para este tipo de aplicación, no se resuelve el problema de comprimir el flujo de tráfico general que circula por una red, puesto que la mayoría de aplicaciones de red no comprimen los datos que generan.

La compresión en el dispositivo tiene lugar en una capa de red mucho más baja, como es la capa de enlace de datos. En el dispositivo, la compresión se efectúa sobre los paquetes individuales que se transmiten por un enlace. La compresión se realiza en tiempo real, a medida que los paquetes se envían a través del dispositivo: el remitente comprime un paquete justo antes de enviarlo y el descompresor lo descomprime tan pronto como lo recibe. Esta operación es transparente para los protocolos de red de las capas superiores.

Nociones básicas sobre compresión de datos

Un compresor de datos reconoce la información “redundante” en los datos y genera un conjunto de datos distinto que contiene la menor redundancia posible. La información “redundante” es aquella información que puede derivarse y volver a crearse a partir de los datos actualmente disponibles. Por ejemplo, el funcionamiento de un compresor puede consistir en reconocer patrones de caracteres repetidos en una corriente de datos, y sustituirlos por una secuencia de código más corta que represente a ese patrón. Si el compresor y el descompresor se ponen de acuerdo en cuáles son esas secuencias de código, entonces el descompresor siempre podrá volver a crear los datos originales a partir de los datos comprimidos.

A esta correlación entre las secuencias de datos originales y las secuencias correspondientes a la salida comprimida se la conoce normalmente como ***diccionario de datos***. Estos diccionarios pueden definirse estáticamente (información disponible por el compresor y por el descompresor, basada en la experiencia) o pueden generarse dinámicamente, basándose generalmente en la información que se va a comprimir. Los diccionarios estáticos pueden aplicarse en la mayoría de entornos en los que la naturaleza de los datos a procesar es limitada, conocida, y no son muy efectivos si se usan con compresores de uso general. La mayoría de sistemas de compresión utilizan diccionarios dinámicos, incluidos los diccionarios utilizados en el dispositivo. En un 2212, los diccionarios de datos se basan en el paquete que se procesa actualmente y en los posibles paquetes vistos antes, pero no se puede “ver por anticipado” en la corriente de datos, como sucede cuando la compresión se realiza en otras capas. En los sistemas en que el diccionario de datos se crea dinámicamente y está basado solamente en los datos vistos antes, al diccionario normalmente se le conoce como ***historia***. Los términos historia y diccionario de datos se utilizarán indistintamente en el resto del capítulo,

aunque debe entenderse que en otros entornos una historia es una forma específica de diccionario de datos.

El hecho de que el dispositivo utilice diccionarios dinámicos y de que el compresor y el descompresor deban mantener sincronizados sus diccionarios, significa que la compresión de datos se realiza en una corriente de datos que pasa entre dos puntos finales. De ahí que la compresión en el direccionador sea un proceso orientado a la conexión, donde los puntos finales de la conexión son, a su vez, el compresor y el descompresor. Cuando se arranca el proceso de compresión en la corriente, ambos puntos finales restablecen sus diccionarios de datos a un estado inicial conocido y, después, van actualizando dicho estado a medida que se reciben datos.

La compresión puede efectuarse para cada paquete individual, con lo que las historias se restablecerán antes de procesar cada paquete. Sin embargo, lo normal es que los diccionarios de datos no se restablezcan entre paquetes, lo que quiere decir que las historias se basan no sólo en el contenido del paquete actual, sino también en el contenido de los paquetes vistos antes. Esto suele mejorar la eficacia global de la compresión, puesto que aumenta la cantidad de datos que utiliza el compresor para buscar redundancias a eliminar. Un ejemplo sería el caso de un sistema principal que está “sondeando” a otro sistema principal con IP: se envía una serie de paquetes y, generalmente, cada paquete nuevo es casi idéntico al anterior. El compresor puede tener pocas posibilidades a la hora de comprimir el primer paquete, pero reconocerá que cada uno de los paquetes siguientes son muy parecidos al último que se ha enviado y creará versiones muy comprimidas de dichos paquetes.

Puesto que las historias del compresor y del descompresor varían con cada paquete recibido, los mecanismos de descompresión son sensibles a los paquetes perdidos, corrompidos o reordenados. Los protocolos de compresión empleados por el dispositivo incluyen mecanismos de señalización de forma que el compresor y el descompresor pueden detectar una pérdida de sincronización y volver a sincronizarse entre ellos, lo que puede ser necesario si un paquete se pierde debido a un error de transmisión. Generalmente, esto se consigue incluyendo un número de secuencia en cada paquete, que el descompresor comprobará para asegurarse de que está recibiendo todos los paquetes y de que los está recibiendo en orden. Si detecta un error, él mismo se restablecerá a un estado inicial conocido, enviará un señal al compresor para que haga lo mismo y, a continuación, esperará (descartando todos los paquetes que lleguen comprimidos) hasta que el compresor le envíe un acuse de recibo conforme él también se ha restablecido.

La compresión en un enlace suele realizarse con datos que se transmiten en ambos sentidos del enlace. Normalmente, en cada extremo de la conexión funciona tanto un compresor como un descompresor, que se comunican con sus análogos del otro extremo de la conexión, como se muestra en la Figura 20 en la página 234. La salida (compresión) se ejecuta independientemente de la entrada (descompresión). Es posible que se utilicen algoritmos de compresión totalmente diferentes en cada sentido del enlace. Al establecer la conexión de un enlace, el protocolo de control de compresión del enlace negociará con su igual para determinar los algoritmos de compresión que se utilizarán para la conexión. Si los dos puntos finales no pueden ponerse de acuerdo sobre los protocolos de compresión a utilizar, no se realizará ninguna clase de compresión y el enlace funcionará normalmente (los paquetes se enviarán sin comprimir).

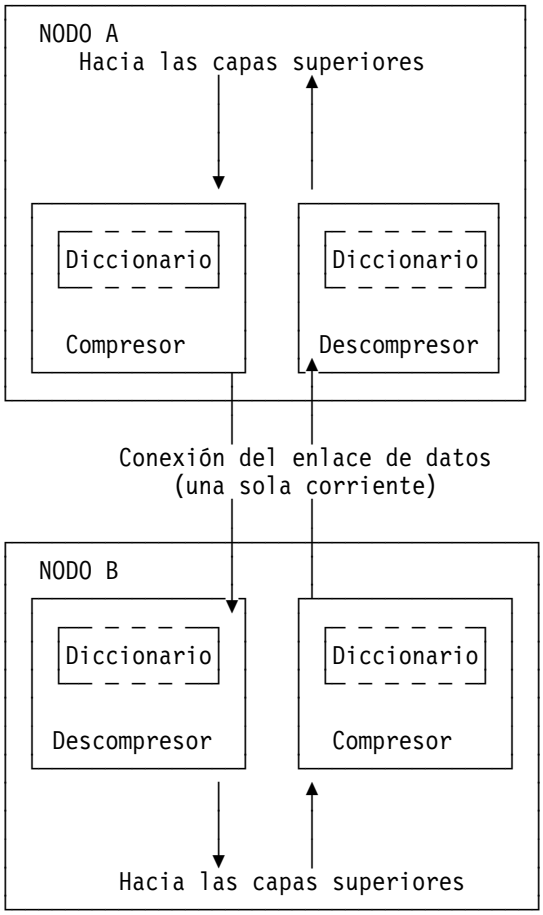


Figura 20. Ejemplo de compresión de datos bidireccional con diccionarios de datos

En realidad, una corriente representa una conexión entre un proceso de compresión específico en un extremo del enlace y un proceso de descompresión asociado en el otro extremo del enlace, lo que es más preciso que decir que es simplemente una “conexión” entre dos nodos; es posible que un protocolo de compresión sofisticado pueda dividir el flujo de datos entre dos sistemas principales en varias corrientes, comprimiendo cada una de forma independiente. Por ejemplo, el CCP de la interfaz PPP es capaz de negociar la utilización de varias historias a través de un solo enlace PPP, aunque el direccionador no dé soporte a esto.

Consideraciones

Tomar la decisión de utilizar o no utilizar compresión de datos no siempre es fácil. 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 que requiere muchos cálculos. A medida que la cantidad de datos procesados aumenta (por unidad de tiempo), más carga de trabajo recae sobre el procesador del dispositivo. Si la carga se vuelve demasiado grande, el rendimiento del dispositivo se degradará (para todas las interfaces de red, no sólo para las que estén utilizando compresión).

En realidad, el dispositivo contiene varios procesadores y utiliza multiproceso asimétrico (por ejemplo, los controladores de E/S del enlace trabajan conjuntamente con el procesador principal), de forma que el efecto de la carga del procesador no siempre podrá medirse inmediatamente. Puesto que la operación de compresión puede solaparse con la transmisión de los paquetes, la carga puede, de hecho, ser totalmente transparente y no plantear ningún problema. No obstante, es posible que el procesador del dispositivo se sobrecargue y que se degrade el rendimiento.

Como norma general, la compresión sólo debe habilitarse en enlaces WAN de baja velocidad (probablemente sólo en enlaces de hasta 64 kilobits por segundo, la velocidad típica de un enlace de marcación RDSI). El ancho de banda total para los datos comprimidos en todos los enlaces probablemente deberá limitarse a varios cientos de kilobits por segundo. No es una buena idea ejecutar la compresión en todos los canales de un adaptador de acceso primario RDSI.

Los parámetros del subsistema de codificación permiten limitar el número de conexiones que ejecutarán concurrentemente la compresión. Pueden habilitarse más interfaces para compresión que las que se están ejecutando realmente. Cuando se alcanza el número máximo de conexiones activas que utilizan compresión, las conexiones adicionales sencillamente no negociarán el uso de la compresión, al menos hasta que no concluya un enlace que ya esté utilizando compresión.

Ocupación de la memoria

Otra cuestión a tener en cuenta cuando se configura la compresión son las necesidades de memoria. Las historias de compresión y descompresión ocupan una cantidad de memoria importante, que es un recurso limitado del dispositivo. El algoritmo Stac-LZS, por ejemplo, necesita unos 16 KB para una historia de compresión y unos 8 KB para una historia de descompresión. Este problema aumenta ya que deben existir historias para cada conexión que se establezca: una historia de compresión se sincroniza con su historia de descompresión correspondiente en un direccionador igual. Para un enlace PPP, esto implica una historia de compresión y una historia de descompresión (suponiendo que la compresión de datos se ejecute bidireccionalmente en el enlace). Para un enlace Frame Relay, pueden existir tantas historias como se necesiten, un par para cada conexión virtual (DLCI) que se establezca.

Al arrancar, el dispositivo crea una agrupación de historias de compresión y descompresión. Siempre se asignan a pares y se conocen como ***sesiones de compresión*** (una sesión es simplemente una historia de compresión emparejada con una historia de descompresión). Técnicamente, la compresión y la descompresión son funciones independientes, pero en la práctica, la compresión casi siempre se ejecuta bidireccionalmente, así que, para simplificar el funcionamiento, la memoria se gestiona y se configura en términos de sesiones más que de historias individuales. Puesto que cada algoritmo de compresión tiene necesidades de memoria distintas, tanto para la compresión como para la descompresión, para poder manejar el caso peor se asigna un tamaño de sesión de aproximadamente 30 KB. La agrupación de sesiones de compresión se llena según las opciones configuradas en el subsistema de codificación. Consulte el Capítulo 13, “Configuración y supervisión del subsistema de codificación” en la página 223 para obtener más detalles.

Cuando el dispositivo intente establecer una conexión de compresión en un enlace, empezará por reservar una sesión de la agrupación de sesiones asignadas. Si no hay sesiones disponibles, la compresión no se efectuará en esta conexión. El direccionador intentará iniciar la compresión en esta conexión más adelante, cuando haya sesiones disponibles.

El número de sesiones de compresión asignadas es un parámetro configurable. Al establecer el número de sesiones asignadas, se limita la cantidad de memoria utilizada y el número máximo de conexiones que pueden funcionar simultáneamente con compresión. Limitar el número de conexiones que pueden funcionar simultáneamente con compresión permite controlar el problema de la carga de la CPU.

Contenido de los datos

Debe tenerse en cuenta la naturaleza real de los datos que se van a transmitir antes de habilitar la compresión para esa conexión. La compresión funciona mejor con ciertos tipos de datos que en otros. Los paquetes que contienen mucha información casi idéntica (por ejemplo, el conjunto de paquetes generados por un mandato "ping" de IP) normalmente se pueden comprimir muy bien. Una colección aleatoria típica de texto y datos binarios que se transmita por un enlace se suele poder comprimir en una proporción que va de 1,5:1 a 3:1. Algunos datos sencillamente no pueden comprimirse. En particular, los datos que ya se han comprimido, raramente podrán comprimirse más. De hecho, los datos que ya se han comprimido antes, puede que se expandan al enviarlos al motor de compresión.

Si se sabe por adelantado que la mayor parte del flujo de datos que pasará por una conexión consistirá en datos comprimidos, entonces es recomendable no habilitar la compresión para esta conexión. Un ejemplo de esto es una conexión con un sistema principal que esté configurado fundamentalmente como sede de archivos FTP, donde todos los archivos disponibles para ser transmitidos están almacenados en el sistema principal en algún formato comprimido.

Compresión en la capa de enlace

Un último factor a tener en cuenta es la naturaleza del enlace de red entre los dos sistemas principales. La compresión puede realizarse en una capa incluso más baja que la de las interfaces hardware del dispositivo. En concreto, el hardware y el firmware de muchos módems modernos incorporan mecanismos de compresión de datos. Si la compresión se va a realizar en el enlace, en la capa más baja (fuera del dispositivo), lo mejor será no habilitar la compresión de datos en el dispositivo para esta interfaz. Como ya se ha mencionado, comprimir una corriente de datos ya comprimidos no suele ser efectivo y, de hecho, puede degradar ligeramente el rendimiento. A menos que haya una razón concreta para creer que el direccionador hará un mejor trabajo de compresión que el hardware del enlace, lo mejor es dejar que sea éste último el que realice la compresión.

Configuración y supervisión de la compresión de datos para enlaces PPP

El 2212 utiliza el protocolo de control de compresión (CCP) para PPP para negociar la utilización de la compresión en un enlace. El CCP proporciona un mecanismo general para negociar la utilización de un protocolo de compresión determinado, incluso, posiblemente, la utilización de protocolos distintos en cada sentido del enlace y varias opciones específicas del protocolo. El software soporta los protocolos Stac-LZS y MPPC, de forma que el igual también debe dar soporte al menos a uno de estos algoritmos para que la negociación sobre la compresión de datos entre los dos nodos sea satisfactoria. Los dos nodos también deben ponerse de acuerdo sobre las opciones específicas del algoritmo para que funcione la compresión.

Configuración de la compresión de datos para enlaces PPP

Para configurar la compresión de datos para enlaces PPP:

1. Habilite el protocolo CCP para el enlace con el mandato **enable ccp**. Esto permite que el enlace negocie qué tipo de compresión utilizar con el otro nodo. En la negociación se acuerda el algoritmo de compresión que se utilizará, así como las opciones específicas del protocolo.
2. Seleccione los algoritmos de compresión que pueden negociarse, utilizando el mandato **set ccp algorithms**.
3. Establezca los parámetros negociables para cada algoritmo de compresión, utilizando el mandato **set ccp options**.

Se puede visualizar la configuración actual de compresión con el mandato **list ccp**.

En la Tabla 22 se listan los mandatos disponibles y la Figura 21 es un ejemplo de cómo configurar la compresión para un enlace PPP. Para obtener descripciones detalladas de estos mandatos, consulte el apartado 'Mandatos de configuración punto a punto', de la publicación *Software de Access Integration Services Guía del usuario*.

Tabla 22. Mandatos de configuración de la compresión de datos para PPP

Mandato de compresión de datos	Acción
disable ccp	Inhabilita la compresión de datos.
enable ccp	Habilita la compresión de datos.
set ccp options	Establece las opciones del algoritmo de compresión.
set ccp algorithms	Especifica una lista de algoritmos de compresión, ordenados por prioridad.
list ccp	Muestra 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 para 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, deberá utilizar el mandato **encapsulator** para acceder al menú de configuración PPP.
2. Si se habilita CCP y no establece ningún algoritmo para el enlace, el software configurará automáticamente el enlace para que utilice los protocolos STAC y MPPC, como si se hubiera entrado el mandato **set ccp algorithms stac mppc**.

   Si se establecen varios algoritmos, el orden de los algoritmos determinará su preferencia a la hora de negociar con ellos para el enlace.

   Si ejecuta el mandato **set ccp algorithms none**, el software inhabilitará automáticamente la compresión para el enlace.

   Si MPPE y CCP están habilitados, el algoritmo de compresión es MPPC.

Supervisión de la compresión de datos para enlaces PPP

La compresión se supervisa de la misma forma que los otros componentes PPP. En el apartado 'Acceso a la interfaz del proceso de supervisión', de la publicación *Software de Access Integration Services Guía del usuario*, se describe cómo acceder al entorno de la consola PPP y se describen detalladamente los mandatos. En la Tabla 23 se listan los mandatos relativos a la compresión. En la Figura 22 en la página 239 se muestra un ejemplo de listado con información sobre la compresión para una interfaz PPP.

Tabla 23. Mandatos de supervisión de la compresión de datos para PPP

Mandato	Función
list control ccp	Lista el estado del CCP y de las opciones negociadas.
list ccp	Lista las estadísticas de los paquetes del CCP.
list cdp o **list compression**	Lista las estadísticas de los datagramas comprimidos.

```
+ 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 para una interfaz PPP

Configuración y supervisión de la compresión de datos para enlaces Frame Relay

Después de configurar los parámetros de compresión globales y de habilitar la compresión para la interfaz, deberá establecer los parámetros para cada uno de los circuitos (PVC) de la interfaz Frame Relay. Cada circuito definido para la interfaz puede tener habilitada la compresión y cada circuito que negocie satisfactoriamente la utilización de la compresión utilizará una sesión de compresión de la agrupación global. También puede inhabilitar la compresión para la interfaz, lo que quiere decir que ningún circuito de la interfaz será elegible para transportar tráfico de datos comprimidos.

Configuración de la compresión de datos para enlaces Frame Relay

Para configurar la compresión de datos para enlaces FR:

1. Habilite la compresión para la interfaz ejecutando el mandato **enable compression**. Esto habilita el enlace para que negocie la compresión con el otro nodo.
2. Habilite la compresión para cada nuevo PVC que vaya a transportar datos comprimidos con el mandato **add permanent-virtual-circuit**. Se pueden cambiar los circuitos PVC existentes utilizando el mandato **change permanent-virtual-circuit**.

Se puede visualizar la configuración actual de compresión ejecutando los mandatos **list lmi** o **list permanent-virtual-circuit**.

En la Tabla 24 en la página 241 se listan los mandatos disponibles para configurar la compresión para un enlace Frame Relay y la Figura 23 es un ejemplo de configuración de un enlace Frame Relay. Hallará más información en el apartado "Mandatos de configuración de Frame Relay", de la publicación *Software de Access Integration Services Guía del usuario.*

```
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               Circuit   Circuit     CIR    Burst  Excess
             Name                 Number     Type      in bps  Size   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 para un enlace Frame Relay

Tabla 24. Mandatos de configuración de la compresión de datos

Mandato	Acción
add permanent-virtual-circuit *número*	Utilícelo para habilitar la compresión de datos en un PVC concreto definido para una interfaz.
change permanent-virtual-circuit *número*	Utilícelo para establecer si un PVC específico comprimirá datos o no.
disable compression	Inhabilita la compresión de datos.
enable compression	Habilita la compresión de datos.
list lmi	Muestra la configuración actual de la interfaz.
list permanent	Muestra información resumida sobre los circuitos.

Nota: Si se habilita la compresión para circuitos huérfanos, se reducirá el número de sesiones de compresión disponibles para los PVC nativos en el dispositivo.

Si se habilita la compresión para una interfaz Frame Relay que ya tiene habilitada la compresión, el software le pedirá si quiere cambiar los parámetros de compresión de la interfaz, como se muestra en el ejemplo siguiente. Se puede cambiar la compresión de la interfaz sin inhabilitar la compresión.

Ejemplo de cambio de la compresión para 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 para enlaces Frame Relay

La compresión se supervisa de la misma forma que los otros componentes de Frame Relay. En el apartado "Mandatos de supervisión de Frame Relay", de la publicación *Software de Access Integration Services Guía del usuario* se describe cómo acceder al entorno de la consola Frame Relay y se describen detalladamente los mandatos. En la Tabla 25 se listan los mandatos relativos a la compresión. En "Ejemplo: Supervisión de la compresión para una interfaz o circuito Frame Relay" en la página 242 se muestra un ejemplo de listado con información sobre la compresión para una interfaz Frame Relay.

Tabla 25. Mandatos de supervisión de la compresión de datos para Frame Relay

Mandato	Se muestra
list lmi	Muestra el estado actual de la interfaz.
list permanent	Muestra información resumida sobre los circuitos.
list circuit	Muestra el estado actual de un circuito.

Ejemplo: Supervisión de la compresión para 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                                  Orphan  Type/   Frames      Frames
 Number            Circuit Name           Circuit State Transmitted  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
```

Capítulo 15. Utilización de la autenticación local o remota

La autenticación es el proceso de determinar quién es un determinado usuario (o entidad). Autenticar el acceso de los usuarios para el protocolo PPP en el 2212 aumenta la flexibilidad de la gestión de perfiles de usuario en lo que se refiere a los protocolos PPP de autenticación: PAP, MSCHAP, CHAP y SPAP. Consulte el apartado 'Protocolos de autenticación PPP', de la publicación *Software de Access Integration Services Guía del usuario*, para obtener información adicional sobre cómo configurar los protocolos PAP, MSCHAP, CHAP y SPAP.

La autenticación puede configurarse localmente o puede configurarse para consolidar la configuración de usuarios utilizando servidores de autenticación disponibles en la red para atender a las peticiones de autenticación provenientes de toda la red. El IBM 2212 implementa un sistema de autenticación que se mantiene de forma local, así como los protocolos de servidor de autenticación siguientes:

- Radius
- TACACS
- TACACS+

Utilización de la seguridad de autenticación, autorización y contabilidad (AAA)

La seguridad de autenticación, autorización y contabilidad (AAA) consiste en protocolos configurables que permiten controlar el acceso a los servicios. Se puede configurar la AAA para que realice la autenticación de forma local o remota.

Los protocolos de seguridad pueden configurarse para tres tipos de funciones.

- Enlaces PPP
- Inicio de sesión de usuarios (inicio de sesión Telnet o Consola)
- Túneles

La configuración se realiza definiendo un servidor principal y uno secundario. La información del servidor se configura y almacena de forma independiente de la configuración AAA. El nombre del perfil del servidor que se utilizará se proporciona durante la configuración.

La contabilidad no puede realizarse localmente bajo ninguna circunstancia y debe ser Radius o TACACS+.

La autorización sólo puede realizarse localmente o mediante autenticación remota, utilizando Radius o TACACS+.

¿Qué es la seguridad AAA?

La seguridad AAA es el nombre del sistema de seguridad de este dispositivo. Consta de:

Autenticación
: Proceso de identificación de un usuario. La autenticación utiliza un nombre y una contraseña para permitir el acceso.

Autorización
Proceso de determinación de los servicios a los que un usuario puede acceder. El proceso de autorización puede detectar que el usuario no está autenticado. En este caso, el agente de autorización determinará si se permite que el usuario sin autenticar puede acceder a los servicios en cuestión.

Contabilidad
Proceso por el que se registra cuándo un usuario ha iniciado o finalizado una sesión. Existen dos tipos de registros de contabilidad.

Registros de inicio
Indican que se va a iniciar un servicio.

Registros de finalización
Indican que un servicio ha finalizado.

Utilización de PPP

Pueden configurarse las funciones siguientes para el protocolo punto a punto (PPP):

- Autenticación
- Autorización
- Contabilidad

Cada función puede tener su propio protocolo de seguridad, que se configurará independientemente.

- La configuración del protocolo de autenticación no afecta a los de autorización o contabilidad.
- La configuración del protocolo de autorización no afecta a los de autenticación o contabilidad.
- La configuración del protocolo de contabilidad no afecta a los de autenticación o autorización.
- Si se configura la seguridad AAA como remota, la autenticación, la autorización y la contabilidad se establecerán como remotas.
- Si se configura la seguridad AAA como local, la autenticación y la autorización se establecerán como locales, y no se tendrá en cuenta la contabilidad. Ni la autenticación ni la autorización se pueden inhabilitar.

Consulte los mandatos de configuración del protocolo punto a punto, en *Software de Access Integration Services Guía del usuario* para obtener más información sobre los mandatos de configuración PPP que pueden utilizarse en este entorno.

Protocolos válidos de seguridad PPP

Estos son los protocolos válidos de seguridad PPP:

Métodos de autenticación
Local, RADIUS, TACACS+, TACACS

Métodos de autorización
Local, RADIUS, TACACS+

Métodos de contabilidad
RADIUS, TACACS+

Tabla 26. Establecer protocolos de seguridad PPP

Acción	Autenticación	Autorización	Contabilidad
set AAA local	local	local	hacer caso omiso
set AAA remote	remota	remota	remota
set AUTHENT local	local	hacer caso omiso	hacer caso omiso
set AUTHOR local	hacer caso omiso	local	hacer caso omiso
set AUTHENT remote	remota	hacer caso omiso	hacer caso omiso
set ACCOUNTING local	no procede	no procede	no procede
set AUTHOR remote	hacer caso omiso	remota	hacer caso omiso
set ACCOUNTING remote	hacer caso omiso	hacer caso omiso	remota
disable ACCOUNTING	hacer caso omiso	hacer caso omiso	inhabilitada
disable AUTHENT	no procede	no procede	no procede
disable AUTHOR	no procede	no procede	no procede

Utilización del inicio de sesión

La configuración del inicio de sesión AAA puede ser remota o local. Si se quiere que la autenticación sea local, la autorización también deber ser local. Si se elige la autenticación remota, la autorización también deber ser remota. No está permitido que la contabilidad sea local, así que si la autenticación y la autorización son locales, la contabilidad debe inhabilitarse.

Atención: Antes de habilitar el inicio de sesión de consola, guarde la configuración con el inicio de sesión de consola inhabilitado. Si la autenticación del inicio de sesión está establecida en un servidor remoto que utiliza Radius, TACACS o TACACS+ y el direccionador no puede acceder al servidor de autenticación, se denegará el acceso al direccionador. Inhabilitar el inicio de sesión de consola evita situaciones de bloqueo.

Si se configura la autenticación remota, se puede establecer la autorización para que utilice el protocolo de autorización remota Radius o TACACS+, y se puede establecer la contabilidad para que utilice Radius o TACACS+.

- Si se configura la seguridad AAA como local, la autenticación y la autorización se establecerán como locales, y la contabilidad se inhabilitará.
- Si se configura la seguridad AAA como remota, la autenticación, la autorización y la contabilidad se establecerán como remotas.
- Si se configura el protocolo de autenticación como local, el protocolo de autorización se establecerá automáticamente como local, y se inhabilitará la contabilidad.
- Si se configura el protocolo de autenticación como remoto, el protocolo de autorización se establecerá automáticamente como remoto solamente si está establecido como local y no se tendrá en cuenta el protocolo de contabilidad.
- Si se configura el protocolo de autorización como remoto, el protocolo de autenticación se establecerá automáticamente como remoto solamente si está establecido como local, y no se tendrá en cuenta el protocolo de contabilidad.

- Si se configura el protocolo de contabilidad como remoto, los protocolos de autenticación y de autorización se establecerán automáticamente como remotos solamente si están establecidos como locales.
- Inhabilitar el protocolo de contabilidad, no afecta a los protocolos de autenticación o de autorización.
- No está permitido inhabilitar la autenticación ni la autorización.

Protocolos válidos de seguridad de inicio de sesión y administración

Estos son los protocolos válidos de seguridad de inicio de sesión y de administración:

Métodos de autenticación y autorización
Local, RADIUS, TACACS Plus

Métodos de contabilidad
RADIUS, TACACS Plus

Tabla 27. Establecer protocolos de seguridad de inicio de sesión

Acción	Autenticación	Autorización	Contabilidad
set AAA local	local	local	inhabilitada
set AAA remote	remota	remota	remota
set AUTHENT local	local	local	inhabilitada
set AUTHOR local	local	local	inhabilitada
set AUTHENT remote	remota	remota, si es local; si no, hacer caso omiso	hacer caso omiso
set AUTHOR remote	remota, si es local; si no, hacer caso omiso	remota	hacer caso omiso
set ACCOUNTING remote	remota, si es local; si no, hacer caso omiso	remota, si es local; si no, hacer caso omiso	remota
disable ACCOUNTING	hacer caso omiso	hacer caso omiso	inhabilitada
disable AUTHEN	no procede	no procede	no procede
disable AUTHOR	no procede	no procede	no procede

Utilización de túneles

Establezca la autenticación de túneles igual que la autorización de túneles. Si se establece la autenticación de túneles como local o como remota, se podrá habilitar la contabilidad. El servidor de autorización y de autenticación debe ser el mismo.

Protocolos válidos de seguridad de túneles

Estos son los protocolos válidos de seguridad de túneles:

Métodos de autenticación y autorización
Local, RADIUS

Métodos de contabilidad
RADIUS, TACACS Plus

Tabla 28. Establecer protocolos de seguridad de túneles

Acción	Autenticación	Autorización	Contabilidad
set AAA local	local	local	hacer caso omiso
set AAA remote	remota	remota	remota
set AUTHENT local	local	local	hacer caso omiso
set Author local	local	local	hacer caso omiso
set AUTHENT remote	remota	remota	hacer caso omiso
set AUTHOR remote	remota	remota	hacer caso omiso
set ACCOUNTING remote	hacer caso omiso	hacer caso omiso	remota
disable ACCOUNTING	hacer caso omiso	hacer caso omiso	inhabilitada
disable AUTHENT	no procede	no procede	no procede
disable AUTHOR	no procede	no procede	no procede

Normas sobre las contraseñas

La autenticación local le permite utilizar una contraseña para controlar el acceso en el inicio de sesión. La contraseña puede comprobarse con alguna o con todas las normas siguientes.

Nota: Las normas siguientes atañen solamente al inicio de sesión de usuarios PPP y no al inicio de sesión de consola.

- Que tenga un número mínimo de caracteres. Defina el número de caracteres obligatorios.
- Que contenga al menos un carácter alfabético.
- Que contenga al menos un carácter no alfabético.
- Que contenga un carácter no numérico en la primera posición.
- Que contenga un carácter no numérico en la última posición.
- Que no contenga más de tres caracteres consecutivos idénticos a los utilizados en la contraseña anterior.
- Que no contenga más de dos caracteres consecutivos.
- Que la identificación de usuario no forme parte de la contraseña.
- Que sea diferente de las tres contraseñas anteriores.
- Que se cambie después de cierto número de días. Defina el número de días que tendrán que transcurrir entre cada cambio de contraseña.
- Que se bloquee después de un número determinado de intentos de inicio de sesión erróneos. Defina el número de intentos erróneos.

Explicación de los servidores de autenticación

Un ***servidor de autenticación*** es un servidor de la red dedicado a validar identificaciones de usuario y contraseñas para la red. Si se configura un dispositivo para realizar la autenticación mediante un servidor de autenticación y el

dispositivo recibe un paquete de un protocolo de autenticación, el dispositivo envía una identificación de usuario y una contraseña al servidor para su autenticación. Si la identificación de usuario y la contraseña son correctas, el servidor responde positivamente. El dispositivo podrá comunicarse con el remitente de la petición. Si el servidor no encuentra la identificación de usuario ni la contraseña recibidas del dispositivo, le responderá negativamente. El dispositivo rechazará la sesión de la que recibió la petición de autenticación.

Soporte de identificación de seguridad

El 2212 puede autenticar clientes de acceso telefónico que utilicen la identificación de seguridad con un servidor ACE/Server de Security Dynamics. El servidor ACE/Server utiliza los métodos TACACS, TACACS+ o RADIUS para autenticar el cliente. Configure el cliente de acceso telefónico como los demás clientes de acceso telefónico del 2212.

El cliente de acceso telefónico iniciará la sesión como siempre, pero utilizará el código de paso de la identificación de seguridad como contraseña. El código de paso de la identificación de seguridad consiste en un número PIN de 4 a n dígitos, seguido del número de identificación de seguridad proporcionado por la tarjeta de señas. (El número máximo de dígitos del PIN depende del servidor). La identificación de usuario y la contraseña podrían ser los siguientes:

```
Username: | John Customer      |

Password: | 1234098765         |
```

Figura 24. Nombre de usuario y código de paso de la identificación de seguridad

Cuando el servidor ACE/Server autentica el inicio de sesión, es posible que solicite la seña siguiente del cliente. La seña siguiente es la seña siguiente de la tarjeta de señas. El número máximo de dígitos de la seña siguiente depende de la tarjeta de señas de identificación de seguridad que esté utilizando el cliente. El cliente podrá entrar el código de paso y la seña siguiente cuando se le solicite la contraseña, utilizando el formato `código de paso*seña`, tal como se muestra en el ejemplo siguiente:

```
Username: | John Customer      |

Password: | 1234098765*111111  |
```

Figura 25. Código de paso de la identificación de seguridad con la seña siguiente

Nota: Cuando el servidor solicita que el cliente entre la seña siguiente, el cliente deberá:

1. Entrar el PIN
2. Esperar una nueva seña de la tarjeta y entrar la seña
3. Escribir un * seguido de la seña siguiente de la tarjeta

El administrador del servidor ACE/Server configura las condiciones que harán que el servidor solicite la seña siguiente o un PIN nuevo.

Los clientes de acceso telefónico deben utilizar SPAP para poder recibir alertas del sistema de autenticación cuando sea necesario que entren la seña siguiente. Si el cliente no utiliza SPAP y no puede conectarse, deberá intentar entrar un código de paso nuevo utilizando el formato `código de paso*seña`. Si el cliente sigue sin poder conectarse, podría haber algún otro problema entre el cliente y el servidor ACE/Server.

Limitaciones

Existen las limitaciones siguientes:

- No se da soporte a los métodos de cifrado Security Dynamics Inc. (SDI) ni DES.
- No se da soporte a la función "New PIN" de la identificación de seguridad.
- TACACS no da soporte a las funciones "New PIN" ni "Next-Token". El cliente puede especificar una seña siguiente al iniciar la sesión, pero el servidor no la utilizará.
- No se da soporte a los clientes configurados para utilizar devolución de llamada.
- Si se utiliza CHAP con TACACS o TACACS+, establezca en 0 el intervalo de repetición de identificación del CHAP.
- No utilice CHAP si utiliza el método de autenticación RADIUS.
- Los clientes conseguirán los mejores resultados utilizando TACACS+ y SPAP.
- No se da soporte a los clientes DIAL de Windows 3.1 con autenticación mediante identificación de seguridad que utilice multienlace.
- Si se utiliza la autenticación mediante identificación de seguridad, lo más recomendable es utilizar el software de cliente más reciente (por ejemplo, Windows 95 u OS/2).

Utilización de la autenticación local o remota

Capítulo 16. Configuración de la autenticación

Este capítulo describe los mandatos operativos y de configuración para la autenticación. Consta de los apartados siguientes:

- "Acceso al indicador de configuración de la autenticación"
- "Mandatos de configuración de la autenticación"

Acceso al indicador de configuración de la 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 la autenticación

La Tabla 29 lista los mandatos disponibles en el indicador `Authent config >`.

Tabla 29. Mandatos de configuración de la autenticación

Mandato	Función
? (Ayuda)	Visualiza todos los mandatos disponibles para este nivel de mandato, o lista las opciones de mandatos específicos (si es que están disponibles). Consulte "Obtención de ayuda" en la página xxv.
Disable	Inhabilita la contabilidad para 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 PPP.
Password-rules	Configura las normas de contraseña (habilita o inhabilita).
PPP	Configura AAA para PPP.
Quickset	Configura rápidamente el método de autenticación.
Servers	Configura servidores AAA individuales remotos.
Set	Configura los parámetros de Autenticación independientemente del tipo.
Tunnel	Configura AAA para túneles L2TP.
User-profile	Configura usuarios PPP locales.
Exit	Hace volver al nivel de mandato anterior. Consulte "Salida de un entorno de nivel inferior" en la página xxv.

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

Configuración de la autenticación

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 30 lista los submandatos disponibles con el mandato **login**.

Tabla 30. Submandatos de login

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	Establece los parámetros de configuración de AAA para el inicio de sesión.

Disable

Utilice el mandato **login disable** para inhabilitar la contabilidad.

Sintaxis:

lo**gin disable** accounting

List

Utilice el mandato **login list** para visualizar los parámetros de configuración de AAA.

Configuración de la autenticación

Sintaxis:

lo**gin list** all
accounting
authentication
authorization
config

Set

Utilice el mandato **login set** para configurar los parámetros de autenticación.

Sintaxis:

lo**gin set** aaa
accounting
authentication
authorization

aaa *tipoaut*
Establece el tipo de autenticación, autorización y contabilidad. *Tipoaut* es uno de los siguientes:

local Establece el tipo de autenticación, autorización y contabilidad para utilizar una base de datos de usuarios mantenida localmente.

remote
Establece el tipo de autenticación, autorización y contabilidad para utilizar una base de datos de usuarios remota.

server id
Especifica el identificador de la base de datos remota.

accounting *tipoaut*
Establece el tipo de contabilidad. *Tipoaut* es uno de los siguientes:

remote
Establece el tipo de autenticación para utilizar una base de datos de usuarios remota.

server id
Especifica el identificador de la base de datos remota.

authentication *tipoaut*
Establece el tipo de autenticación. *Tipoaut* es uno de los siguientes:

local Establece el tipo de autenticación para utilizar una base de datos de usuarios mantenida localmente.

remote
Establece el tipo de autenticación para utilizar una base de datos de usuarios remota.

server id
Especifica el identificador de la base de datos remota.

authorization *tipoaut*
Establece el tipo de autorización. *Tipoaut* es uno de los siguientes:

local Establece el tipo de autorización para utilizar una base de datos de usuarios mantenida localmente.

remote
Establece el tipo de autorización para utilizar una base de datos de usuarios 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 en cada interfaz PPP.

Sintaxis:

n**ets-info**

Password-rules

Utilice el mandato **password-rules** para configurar la contraseña (habilitar o inhabilitar).

La Tabla 31 lista los submandatos disponibles con el mandato **password-rules**.

Tabla 31. Submandatos de login

Mandato	Función
Disable	Inhabilita una norma de contraseña.
Enable	Habilita una norma de contraseña.
List	Muestra el estado actual de las normas de contraseña (habilitado o inhabilitado).

Disable

Utilice el mandato **password-rules disable** para inhabilitar cualquiera o todas las normas de contraseña.

Sintaxis:

p**assword-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

compare-ident-prev
Compara la identidad del usuario anterior con el usuario que solicita un cambio de contraseña.

change-days
El número máximo de días antes de que se solicite un cambio de contraseña.

Valores válidos: del 0 al 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 puede contener más de 3 caracteres utilizados en una contraseña anterior en la misma posición.

last-non-numeric
El último carácter de la contraseña no puede ser numérico.

Valores válidos: cualquier carácter no numérico

Valor por omisión: ninguno

lockout
El número de veces que se puede intentar entrar una contraseña antes de que se bloquee.

Valores válidos: del 0 al 360

Valor por omisión: 3

minimum-length
El número mínimo de caracteres necesario para tener una contraseña válida.

Valores válidos: del 1 al 31

Valor por omisión: 8

maximum-length
El número máximo de caracteres que puede contener una contraseña.

Valores válidos: del 1 al 31

Valor por omisión: 8

one-alpha
Al menos uno de los caracteres de la contraseña debe ser alfanumérico.

one-nonalpha
Al menos uno de los caracteres de la contraseña debe ser numérico.

prev-three
La contraseña no puede ser igual que una de las tres últimas contraseñas.

userid-contained
La contraseña no puede contener el id de usuario como parte de la contraseña.

Enable

Utilice el mandato **password-rules enable** para habilitar cualquiera o todas las normas de contraseña. Consulte el mandato **disable** para ver una lista con las descripciones de las normas 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 visualizar el estado actual de las normas de contraseña (habilitado o inhabilitado).

Sintaxis:

password-rules list

PPP

Utilice el mandato **ppp** para configurar AAA para PPP.

La Tabla 32 lista los submandatos disponibles con el mandato **ppp**.

Tabla 32. Submandatos de PPP

Mandato	Función
Disable	Inhabilita la contabililidad para PPP.
List	Muestra los parámetros de configuración de AAA para PPP.
Set	Establece los parámetros de configuración de AAA para PPP.

Disable

Utilice el mandato **ppp disable** para inhabilitar la contabilidad para PPP.

Sintaxis:

ppp disable accounting

List

Utilice el mandato **ppp list** para visualizar los parámetros de configuración de AAA para PPP.

Sintaxis:

ppp list all
accounting
authentication

authorization

config

Set

Utilice el mandato **ppp set** para establecer los parámetros de configuración de AAA para PPP.

Sintaxis:

ppp set aaa

accounting

authentication

authorization

aaa *tipoaut*

Establece el tipo de autenticación, autorización y contabilidad. *Tipoaut* es uno de los siguientes:

local Establece el tipo de autenticación, autorización y contabilidad para utilizar una base de datos de usuarios mantenida localmente.

remote

Establece el tipo de autenticación, autorización y contabilidad para utilizar una base de datos de usuarios remota.

server id

Especifica el identificador de la base de datos remota.

accounting *tipoaut*

Establece el tipo de contabilidad. *Tipoaut* es uno de los siguientes:

remote

Establece el tipo de autenticación para utilizar una base de datos de usuarios remota.

server id

Especifica el identificador de la base de datos remota.

authentication *tipoaut*

Establece el tipo de autenticación. *Tipoaut* es uno de los siguientes:

local Establece el tipo de autenticación para utilizar una base de datos de usuarios mantenida localmente.

remote

Establece el tipo de autenticación para utilizar una base de datos de usuarios remota.

server id

Especifica el identificador de la base de datos remota.

authorization *tipoaut*

Establece el tipo de autorización. *Tipoaut* es uno de los siguientes:

local Establece el tipo de autorización para utilizar una base de datos de usuarios mantenida localmente.

remote

Establece el tipo de autorización para utilizar una base de datos de usuarios remota.

server id

Especifica el identificador de la base de datos remota.

Servers

Utilice el mandato **servers** para configurar servidores remotos individuales de AAA.

La Tabla 33 lista los submandatos disponibles con el mandato **servers**.

Tabla 33. Submandatos de Server

Mandato	Función
Add	Añade un perfil de servidor remoto de AAA.
Change	Cambia un perfil de servidor remoto.
Delete	Suprime un perfil de servidor remoto.
Lists	Muestra la información de perfil de servidor de AAA.

Add

Utilice el mandato **servers add** para añadir un perfil de servidor remoto.

Sintaxis:

ser**vers add** nombre

radius Establece el tipo de autenticación para utilizar el protocolo RADIUS del servidor de autenticación.

Se pueden establecer valores para los siguientes parámetros:

key-for-encryption:
Especifica la clave de cifrado.

Valores válidos: Cualquier serie de caracteres alfanumérica de hasta 32 caracteres.

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: del 1 al 100

Valor por omisión: 3

retry-interval

Valores válidos: del 1 al 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

Author-Authent
Especifica si se deben transferir los atributos de autorización durante la autenticación.

Valores válidos: yes, no

Valor por omisión: yes

tacacs Establece el tipo de autenticación para utilizar el protocolo TACACS del servidor de autenticación.

Se pueden establecer valores para 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: del 1 al 100

Valor por omisión: 3

retry-interval

Valores válidos: del 1 al 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
Establece el tipo de autenticación para utilizar el protocolo TACACS+ del servidor de autenticación.

Se pueden establecer valores para 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 utilizará.

Valores válidos: Cualquier valor de 16 dígitos hexadecimales

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: del 0 al 15

Valor por omisión: 0

restarts
Establece el número de reinicios. Este parámetro no incluye los reinicios de tiempo excedido y se refiere a los reinicios solicitados por el servidor.

Valores válidos: del 0 al 3200

Valor por omisión: 0

time-to-connect
La cantidad de tiempo permitida para obtener la autenticación del servidor.

Valores válidos: del 1 al 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 cambiar un perfil de servidor remoto. Consulte el mandato **add** para ver las descripciones de perfil de servidor remoto.

Sintaxis:

servers change radius
tacacs
tacacsplus

Consulte el mandato **servers add** para ver las descripciones de perfil de servidor remoto.

Delete

Utilice el mandato **servers delete** para suprimir un perfil de servidor remoto. Consulte el mandato **add** para ver las descripciones de perfil de servidor remoto.

Sintaxis:

servers delete radius
tacacs
tacacsplus

Consulte el mandato **servers add** para ver las descripciones de perfil de servidor remoto.

List

Utilice el mandato **servers list** para visualizar la información de perfil de servidor de AAA.

Sintaxis:

servers list all
names
profile

Set

Utilice el mandato **set** para establecer los parámetros para el inicio de sesión, PPP y el túnel L2TP.

Sintaxis:

set aaa
accounting
authentication
authorization

aaa *tipoaut*
Establece el tipo de autenticación, autorización y contabilidad. *Tipoaut* es uno de los siguientes:

local Establece el tipo de autenticación, autorización y contabilidad para utilizar una base de datos de usuarios mantenida localmente.

remote
Establece el tipo de autenticación, autorización y contabilidad para utilizar una base de datos de usuarios remota.

server id
Especifica el identificador de la base de datos remota.

accounting *tipoaut*
Establece el tipo de contabilidad para el inicio de sesión, PPP y el túnel. *Tipoaut* es uno de los siguientes:

remote
Establece el tipo de autenticación para utilizar una base de datos de usuarios remota.

server id
Especifica el identificador de la base de datos remota.

authentication *tipoaut*
Establece el tipo de autenticación para el inicio de sesión, PPP y el túnel. *Tipoaut* es uno de los siguientes:

local Establece el tipo de autenticación para utilizar una base de datos de usuarios mantenida localmente.

remote
Establece el tipo de autenticación para utilizar una base de datos de usuarios remota.

server id
Especifica el identificador de la base de datos remota.

authorization *tipoaut*
Establece el tipo de autorización para el inicio de sesión, PPP y el túnel. *Tipoaut* es uno de los siguientes:

local Establece el tipo de autorización para utilizar una base de datos de usuarios mantenida localmente.

remote
Establece el tipo de autorización para utilizar una base de datos de usuarios 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 34 lista los submandatos disponibles con el mandato **tunnel**.

Tabla 34. Submandatos de tunnel

Mandato	Función
Disable	Inhabilita la contabilidad para el túnel L2TP.
List	Visualiza los parámetros de configuración de AAA para el túnel L2TP.
Set	Establece 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:

t**unnel disable** accounting

List

Utilice el mandato **tunnel list** para visualizar los parámetros de AAA para el túnel L2TP.

Sintaxis:

tu**nnel list** all
accounting
authentication
authorization
config

Set

Utilice el mandato **tunnel set** para establecer los parámetros de configuración de AAA para el túnel L2TP.

Sintaxis:

t**unnel set** aaa
accounting
authentication
authorization

aaa *tipoaut*

Establece el tipo de autenticación, autorización y contabilidad. *Tipoaut* es uno de los siguientes:

local Establece el tipo de autenticación, autorización y contabilidad para utilizar una base de datos de usuarios mantenida localmente.

remote

Establece el tipo de autenticación, autorización y contabilidad para utilizar una base de datos de usuarios remota.

server id

Especifica el identificador de la base de datos remota.

Configuración de la autenticación

accounting *tipoaut*

Establece el tipo de contabilidad. *Tipoaut* es uno de los siguientes:

remote

Establece el tipo de autenticación para utilizar una base de datos de usuarios remota.

server id

Especifica el identificador de la base de datos remota.

authentication *tipoaut*

Establece el tipo de autenticación. *Tipoaut* es uno de los siguientes:

local Establece el tipo de autenticación para utilizar una base de datos de usuarios mantenida localmente.

remote

Establece el tipo de autenticación para utilizar una base de datos de usuarios remota.

server id

Especifica el identificador de la base de datos remota.

authorization *tipoaut*

Establece el tipo de autorización. *Tipoaut* es uno de los siguientes:

local Establece el tipo de autorización para utilizar una base de datos de usuarios mantenida localmente.

remote

Establece el tipo de autorización para utilizar una base de datos de usuarios 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 podrá acceder a los siguientes mandatos.

Tabla 35. Mandatos de configuración de perfil de usuario

Mandato	Función
? (Ayuda)	Visualiza todos los mandatos disponibles para este nivel de mandato, o lista las opciones de mandatos específicos (si es que están disponibles). Consulte “Obtención de ayuda” en la página xxv.
Add	Añade un perfil de usuario PPP.
Change	Cambia un perfil de usuario PPP.
Delete	Suprime un perfil de usuario PPP.
Disable	Inhabilita un perfil de usuario PPP.
Enable	Habilita un perfil de usuario PPP.
List	Lista la información de perfil de usuario PPP.
Report	Genera un informe de perfiles de usuario PPP.
Reset-user	Restablece un perfil de usuario PPP.
Exit	Hace volver al nivel de mandato anterior. Consulte “Salida de un entorno de nivel inferior” en la página xxv.

Add

Utilice el mandato **user profiles add** para añadir el perfil de usuario de un usuario remoto a la base de datos local de usuarios PPP o para dar un acceso de túnel igual mediante 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 PPP. Puede añadir hasta 500 usuarios. Añada un usuario PPP para cada direccionador remoto o cliente DIALS que se puede conectar al dispositivo que está configurando.

Consulte el apartado Add en el capítulo "El proceso CONFIG (CONFIG - Talk 6) y los mandatos" de la publicación *Software de Access Integration Services Guía del usuario* para obtener una descripción de la sintaxis y las opciones del mandato.

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 Da a un igual acceso de túnel al direccionador mediante una red IP. El igual queda entonces autorizado a iniciar en el direccionador sesiones de PPP por túnel.

Consulte el apartado Add del capítulo "Configuración del proceso CONFIG" de la publicación *Software de Access Integration Services Guía del*

usuario para obtener una descripción de la sintaxis y las opciones del mandato.

Ejemplo:

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

       Tunnel name: tunnel02
          Endpoint: 2.2.2.22
```

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 perfiles 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 la lista.

Valores válidos: name, verb, user, addr, encr, zdump

Valor por omisión: verb

PPP user name
Lista el nombre de usuario.

Expiry Lista la fecha de caducidad.

User IP address
Lista la dirección IP del usuario.

Encryption
Lista si se ha habilitado o no se ha habilitado el cifrado.

Status Lista si se ha habilitado o no se ha habilitado el estado.

Login attempts
Lista el número de veces que el usuario ha intentado iniciar la sesión.

Login failures
Lista el número de intentos fallidos de inicio de sesión.

Lockout attempts
Lista el número de intentos bloqueados.

Report

Utilice el mandato **report** para generar un informe de perfiles de usuario 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 alotted
-----------------  -------------------
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:

res**et-user** *nombre*

Capítulo 17. Utilización y configuración de los protocolos de cifrado

Nota: El soporte de cifrado es opcional y debe añadirse a la carga de software mediante el mandato **load add**. Consulte el Mandato **load** del proceso CONFIG, en *Software de Access Integration Services Guía del usuario*.

El uso del cifrado múltiple (utilizar el cifrado tanto en la capa de seguridad IP como en la capa de enlace de datos PPP o Frame Relay) dentro del direccionador está restringido por los reglamentos de exportación del Gobierno de los Estados Unidos. Sólo está soportado en las cargas de software bajo estricto control de exportación (cargas de software que dan soporte a claves RC4 con 128 bits y DES triple).

El objetivo del cifrado es transformar datos a un formato no legible para asegurar la confidencialidad. Los datos ***cifrados*** deben ser descifrados para obtener los datos originales.

El 2212 da soporte a:

- El algoritmo de cifrado RC4 con claves de 40 y 128 bits para MPPE (Microsoft Point-to-Point Encryption) en interfaces PPP.
- El algoritmo DES-CBC (Data Encryption Standard in Cipher Block Chaining Mode) con claves de 56 bits para el soporte del Protocolo de control de cifrado PPP tal como se describe en los documentos RFC 1968 y 1969.
- El CDMF (Commercial Data Masking Facility) que utiliza claves de 40 bits para el Cifrado de Frame Relay. Este soporte está patentado.
- Frame Relay utiliza también el DES triple y una clave de 128 bits.

Cifrado PPP mediante el Protocolo de control del cifrado

ECP (Encryption Control Protocol) se utiliza en el direccionador para negociar el uso del cifrado en los enlaces punto a punto que se comunican mediante el protocolo PPP. El Protocolo de control del cifrado proporciona un mecanismo generalizado para negociar los algoritmos de cifrado y descifrado que se utilizarán en un enlace PPP. Se pueden negociar 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, puesto que el cifrado en una sola dirección supone un riesgo para la seguridad. El enlace se terminará cuando ECP no pueda negociar los algoritmos de cifrado en ambas direcciones.

Configuración del cifrado ECP para PPP

Para configurar el dispositivo para utilizar el cifrado en la capa de enlace de datos, debe:

1. Establecer las claves de cifrado para los dispositivos remotos y las interfaces PPP remotas.

Establecer la clave de cifrado para el dispositivo remoto mediante el mandato **add ppp-user** en el indicador `Config>`. Consulte el mandato **Add** del capítulo "Configuración del proceso CONFIG" de la publicación *Software de Access Integration Services Guía del usuario* para obtener una descripción de la sintaxis y las opciones del mandato.

Establecer la clave de cifrado para la interfaz PPP local con el mandato **enable ecp** (consulte el mandato `PPP Config>` **enable** de talk 6 en la publicación *Software de Access Integration Services Guía del usuario*).

2. Configure los enlaces individuales PPP para utilizar ECP (Encryption Control Protocol) con 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 del cifrado o establecer el nombre que utiliza el dispositivo cuando solicita el cifrado. Para obtener información acerca de:

- La inhabilitación del cifrado, consulte el mandato `PPP Config>` **disable ecp** en la publicación *Software de Access Integration Services Guía del usuario.*
- El cambio de la clave y contraseña de cifrado del usuario, consulte el mandato `Config>` **change ppp-user** en la publicación *Software de Access Integration Services Guía del usuario.*
- El listado de estados de cifrado, consulte el mandato `PPP Config>` **list ecp** en la publicación *Software de Access Integration Services Guía del usuario.*
- El establecimiento del nombre de dispositivo, consulte el mandato `PPP Config>` **set name** en la publicación *Software de Access Integration Services Guía del usuario.*

Supervisión del cifrado ECP para PPP

Puede supervisar los distintos valores de cifrado de las interfaces:

1. Accediendo al indicador de supervisión con el mandato **talk 5**.
2. Seleccionando la interfaz que desea supervisar con el mandato **network**. Este mandato le coloca en el indicador `PPP n>`, donde *n* representa el número de red. Consulte el apartado "Configuración y supervisión de las interfaces del Protocolo punto a punto" de la publicación *Software de Access Integration Services Guía del usuario* para obtener instrucciones acerca del uso del mandato **network**.

Desde este indicador podrá:

- Listar el estado actual del cifrado, la negociación de cifrado más reciente, el tiempo transcurrido desde el cambio de estado del cifrado y los algoritmos que utilizan los encriptadores. (Consulte el mandato **list control ecp** de la publicación *Software de Access Integration Services Guía del usuario.*)
- Listar los paquetes de control del cifrado recibidos y transmitidos en la interfaz. (Consulte el mandato **list ecp** en la publicación *Software de Access Integration Services Guía del usuario.*)
- Listar los paquetes de datos cifrados transmitidos o recibidos en la interfaz. (Consulte el mandato **list edp** en la publicación *Software de Access Integration Services Guía del usuario.*)

Cifrado de punto a punto de Microsoft (MPPE)

El Cifrado de punto a punto de Microsoft (MPPE) permite a las estaciones de trabajo Windows conectadas de forma remota y denominadas clientes DUN

(Dial-Up Networking) de Microsoft cifrar datos que se transmiten a través de un enlace PPP entre las estaciones y el 2212. MPPE se puede utilizar también para cifrar los datos que se transmiten a través de un enlace PPP de direccionador a direccionador. MPPE se negocia siempre en ambas direcciones.

MPPE utiliza algoritmos de claves secretas para realizar el cifrado. En estos algoritmos se utiliza la misma clave tanto para el cifrado como para el descifrado. Esta clave no la configura el usuario, sino que la genera el proceso de negociación MPPE entre las estaciones de trabajo de envío y recepción. Para utilizar MPPE, deberá configurar el protocolo MS-CHAP (Microsoft Challenge/Handshake Authentication Protocol).

Si la interfaz PPP se autentica con MS-CHAP, el direccionador se ejecuta en una "modalidad Microsoft" en la que negociará sólo MPPC si se ha habilitado la compresión y sólo MPPE si se ha habilitado el cifrado. En la "modalidad Microsoft", el direccionador pasa por alto la lista de prioridad de los algoritmos de compresión e inhabilita la negociación ECP.

Configuración de MPPE

Para configurar MPPE, deberá seguir estos pasos para cada interfaz:

1. Configure MS-CHAP. En la publicación *Software de Access Integration Services Guía del usuario*, consulte los apartados "MS-CHAP (Microsoft PPP CHAP Authentication)" y "Configuración y supervisión de las interfaces del Protocolo punto a punto" para obtener información acerca del uso y configuración de MS-CHAP.
2. Si está configurando una conexión de direccionador a direccionador, establezca el nombre de la interfaz PPP local con el mandato **set name** (consulte el mandato `PPP Config>` **set name** en la publicación *Software de Access Integration Services Guía del usuario*).
3. Si quiere utilizar la compresión de datos, habilite MPPC utilizando el mandato **enable ccp** de talk 6 en el indicador `PPP Config>`. MPPE no necesita la compresión de datos.
4. Habilite MPPE. Utilice el mandato **enable mppe** en el indicador `PPP Config>` (consulte el mandato `PPP Config>` **enable** en la publicación *Software de Access Integration Services Guía del usuario*).
5. Reinicie el direccionador para activar la configuración.

También puede inhabilitar MPPE y listar las opciones de MPPE.

- Utilice el mandato **disable mppe** de talk 6 en el indicador `PPP Config>` para inhabilitar MPPE.
- Utilice el mandato **list ccp** de talk 6 en el indicador `PPP Config>` para listar las opciones de MPPE que se han configurado.

Supervisión de MPPE

Active el indicador `PPP>` tal como se describe en el apartado "Supervisión del cifrado ECP para PPP" en la página 272. Utilice el mandato **list mppe** para ver las estadísticas de MPPE y el mandato **list control ccp** para ver el estado de MPPE. En el apartado "Configuración y supervisión de las interfaces del Protocolo punto a punto" de la publicación *Software de Access Integration Services Guía del usuario* encontrará ejemplos de la salida de estos mandatos.

Configuración del cifrado en las interfaces de Frame Relay

Nota: Frame Relay utiliza un esquema de cifrado patentado.

El cifrado de datos está soportado en todas las interfaces en las que haya habilitado el cifrado. Puede configurar circuitos individuales de una interfaz habilitada para el cifrado con el fin de cifrar o no cifrar según se desee.

Para configurar el dispositivo para utilizar el cifrado en enlaces de Frame Relay:

1. Acceda al indicador de configuración de Frame Relay con el mandato **talk 6**.
2. Seleccione la interfaz de Frame Relay que desea que tenga activado el cifrado con el mandato **net** #
3. Habilite el cifrado en la interfaz de Frame Relay utilizando el mandato **enable encryption**. Consulte los mandatos de configuración de Frame Relay en la publicación *Software de Access Integration Services Guía del usuario.*
4. Añada circuitos virtuales permanentes con posibilidad 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 la publicación *Software de Access Integration Services Guía del usuario.*
5. Repita los pasos del 1 al 4 para cada interfaz con posibilidad de cifrado que configure.

Nota: Si el cifrado está activado para un circuito virtual permanente de FR, los datos no fluirán por el circuito a menos que se negocie satisfactoriamente el cifrado con el dispositivo que se encuentre en el otro extremo del circuito virtual. No se da soporte al cifrado para los circuitos huérfanos, ya que se debe configurar el PVC para introducir la clave de cifrado.

También puede inhabilitar el cifrado para una interfaz, cambiar los valores de cifrado para un PVC o listar el estado del cifrado. Para obtener información acerca de

- La inhabilitación del cifrado en una interfaz, consulte el mandato de configuración de Frame Relay **disable encryption** en la publicación *Software de Access Integration Services Guía del usuario.*
- El cambio de los valores de cifrado para un PVC, consulte el mandato de configuración de Frame Relay **change permanent-virtual-circuit** en la publicación *Software de Access Integration Services Guía del usuario.*
- El listado de estados de cifrado, consulte los mandatos de configuración de Frame Relay **list all,**, **list lmi** y **list permanent-virtual-circuit** en la publicación *Software de Access Integration Services Guía del usuario.*

Supervisión del cifrado en las interfaces de Frame Relay

Puede supervisar los distintos valores de cifrado de las interfaces:

1. Accediendo al indicador de supervisión con el mandato **talk 5**.
2. Seleccionando la interfaz que desea supervisar con el mandato **network** #. Este mandato le coloca en el indicador FR x>.

Desde este indicador, puede listar el estado de cifrado actual de una interfaz, un PVC o un circuito. Consulte el mandato de supervisión de Frame Relay **list** en la publicación *Software de Access Integration Services Guía del usuario.*

Capítulo 18. Utilización de la función de política

Este capítulo describe cómo interactúa la función de política con otros componentes de software del direccionador para tomar decisiones acerca de QOS, la seguridad o ambos. También describe los conceptos y mandatos de configuración específicos relacionados con la función de política. Esta función permite la utilización de un servidor de directorios LDAP como depósito central para la información de la política. También se describen los conceptos y pasos de configuración necesarios para habilitar las funciones de LDAP. Los siguientes temas tratan estos conceptos, la manera como los direccionadores aplican las políticas e incluye ejemplos.

- "Visión general de la política"
- "Interacción de la base de datos de políticas y LDAP" en la página 283
- "Generación de normas" en la página 287
- "Ejemplos de configuración" en la página 288

Visión general de la política

La función de política facilita la gestión del tráfico IPv4 en una red. Puede configurar políticas para normas de filtro muy simples (eliminar o pasar) o para casos de seguridad y QOS complejos. La combinación de políticas determina la forma como los direccionadores manejan el tráfico IPv4 en una red.

Decisión y aplicación de una política

La implementación de la política en esta familia de direccionadores constituye la base para las decisiones de política y la forma de aplicarlas. A menudo se hace referencia a estos conceptos como un punto de decisión de política (PDP) y un punto de aplicación de la política (PEP).

La base de datos de políticas, que reside en la memoria del direccionador, consta del conjunto de políticas cargado desde la configuración local y las políticas que se han leído del LDAP. La base de datos de políticas se crea bajo las siguientes condiciones:

- Recarga o reinicio del dispositivo
- Mandato **reset database** de Talk 5
- Renovación automática
- Solicitud de conjunto de SNMP

La base de datos de políticas sirve como PDP y consta de un conjunto de políticas que determinan la manera como los componentes relacionados con la función de política manejan los paquetes. Cuando una política da como resultado una decisión (basada en información como la hora, información del paquete de IP o información especifica del protocolo como puede ser la identificación), la decisión se pasa al componente de aplicación (PEP) para que lleve a cabo la acción. La Figura 26 en la página 276 muestra la relación de estos componentes.

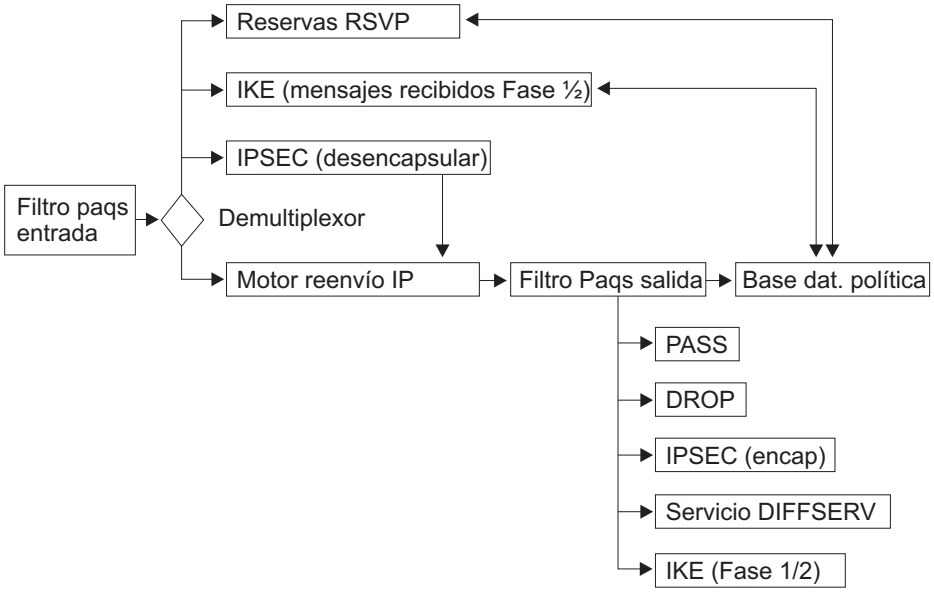


Figura 26. Flujo de paquetes de IP y base de datos de políticas

Decisión de política y flujo de datos

Los Paquetes de IP deben pasar el filtro de paquetes de entrada antes de que se lleve a cabo ninguna otra acción. Si el filtro de paquetes tiene normas presentes, es posible que se lleve a cabo alguna acción en el paquete. Si hay una coincidencia de filtro que excluye el paquete o si no se encuentra ninguna coincidencia en el filtro de paquetes de entrada, se elimina el paquete.

Si el paquete pasa el filtro de paquetes de entrada, va a un filtro de desmultiplexado que comprueba si el paquete tiene un destino local. En caso afirmativo, pasará a otros módulos según el tipo de paquete. 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 esta decisión no rechaza el paquete (el Direccionamiento basado en la política puede decidir rechazarlo), éste va al filtro de paquetes de salida. Si hay normas de filtro en el paquete de salida, es posible que se realice una conversión de dirección (NAT) y puede pasarse o rechazarse. Si no hay normas de filtro, el paquete se pasa. Si hay normas de filtro y no se encuentra ninguna coincidencia, el paquete se rechaza. Si el paquete pasa el filtro de Paquetes de salida, el Motor IP consulta la base de datos de políticas para determinar si se deben llevar a cabo otras acciones en el paquete.

Nota: Si se han habilitado los filtros de paquetes de entrada y salida para las interfaces y se espera que los paquetes que debe controlar la base de datos de políticas atraviesen estas interfaces, tiene que haber una norma de filtro que incluya estos paquetes en los filtros de paquetes de entrada y salida para que no se rechacen antes de consultar la base de datos de políticas. Le sugerimos que utilice la base de datos de políticas para configurar todas las normas de pase/rechazo y no utilizar los filtros de paquetes.

Consultas de políticas de IP

Cuando el motor de reenvío de IP consulta la base de datos de políticas, se pueden devolver los siguientes tipos de combinaciones de decisiones:

- No se ha encontrado ninguna coincidencia—pasar el paquete
- Se ha encontrado una coincidencia—rechazar el paquete
- Se ha encontrado una coincidencia—pasar el paquete
- Se ha encontrado una coincidencia—proteger el paquete en el túnel manual x de IPSec
- Se ha encontrado una coincidencia—proteger el paquete en el túnel x de IPSec de IKE negociado
- Se ha encontrado una coincidencia—iniciar las negociaciones ISAKMP para las fases 1 y 2, rechazar el paquete
- Se ha encontrado una coincidencia—proporcionar DiffServ QOS x, proteger el paquete con IPSec

Consultas de políticas de IPSec

Si IPSec recibe un paquete, primero debe desencapsularlo y decidir después si ha llegado en el túnel IPSec correcto (denominado a veces comprobación de conformidad). Para ello consulta la base de datos de políticas y ésta devuelve los siguientes tipos de decisiones:

- Comprobación de conformidad pasada—reenviar el paquete
- Comprobación de conformidad anómala—rechazar el paquete

Decisiones de políticas de IKE

Es posible que IKE consulte la base de datos de políticas y reciba las decisiones de políticas de IP de la *fase 1* que aparecen en la Tabla 36.

Tabla 36. Consultas de fase 1 de IKE y decisiones recibidas

Tipo de consulta	Decisión
Mensaje 1 (modalidad principal)	No se ha encontrado ninguna coincidencia, rechazar el paquete
Mensaje 1 (modalidad principal)	Se ha encontrado una coincidencia, negociar con la política x de la fase 1
Mensaje 5 (modalidad principal)	No se ha encontrado ninguna coincidencia, detener las negociaciones con el igual, rechazar el paquete
Mensaje 5 (modalidad principal)	No se ha encontrado ninguna coincidencia, detener las negociaciones con el igual, rechazar el paquete
Mensaje 5 (modalidad principal)	Se ha encontrado una coincidencia, la política x coincide, finalizar la fase 1
Mensaje 5 (modalidad principal)	Se ha encontrado una coincidencia, la política y coincide, detener la fase 1 actual e iniciar la fase 1 nueva con la política nueva
Mensaje 1 (modalidad agresiva)	No se ha encontrado ninguna coincidencia, rechazar el paquete
Mensaje 1 (modalidad agresiva)	Se ha encontrado una coincidencia, la política x coincide

Es posible que IKE consulte la base de datos de políticas y reciba las decisiones de políticas de IP de la *fase 2* que aparecen en la Tabla 37 en la página 278.

Tabla 37. Consultas de fase 2 de IKE y decisiones recibidas

Tipo de consulta	Decisión
Mensaje 2 (responder)	No se ha encontrado ninguna coincidencia, rechazar el paquete
Mensaje 2 (responder)	Se ha encontrado una coincidencia, negociar con la política x

Decisiones de políticas de RSVP

Si un paquete es un mensaje de control de RSVP, el RSVP consulta la base de datos de políticas para determinar si debe aceptar o rechazar la reserva. Si se acepta, el RSVP determina los atributos de la reserva que se deben limitar, según 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 se debe asignar y el retardo mínimo que se debe garantizar.

Objetos de política

Una política consta de un perfil, que contiene un conjunto de atributos de paquete sobre los cuales basar las decisiones, acciones que se deben tomar si los atributos de un paquete coinciden con los de un perfil y un período de validez durante el cual se toman las decisiones y se aplican las acciones. Estos elementos se detallan en los siguientes temas:

Las partes que forman una política son objetos nombrados diferenciados. Los objetos de política pueden tener referencias mutuas y, como grupo de elementos relacionados, comprenden una política. Al separar la información de configuración en objetos diferenciados separados, puede volver a utilizar muchos de ellos en definiciones de políticas múltiples, lo que ahorra tiempo y reduce las tareas de mantenimiento. En los temas siguientes se detallan los objetos de política individuales.

Política

El objeto de política describe los condicionales con los que se debe comprobar y, si coinciden, las acciones que se deben realizar. La política hace referencias nombradas al período de validez y el perfil. Para que la política sea válida, estas referencias son obligatorias. La política también debe hacer una referencia nombrada a una o varias de las siguientes acciones: un objeto de túnel con claves manuales de IPSec, una acción IPSec, una acción ISAKMP, una acción RSVP o una acción DiffServ. Son combinaciones válidas:

- Túnel con claves manuales de IPSec
- Acción IPSec para rechazar paquetes
- Acción IPSec para pasar paquetes (sin seguridad)
- Acción IPSec para proteger paquetes, acción ISAKMP
- Acción DiffServ (rechazar)
- Túnel con claves manuales de IPSec y acción DiffServ (pasar)
- Acción IPSec para proteger paquetes, acción ISAKMP, acción DiffServ (pasar)
- Acción RSVP
- Acción RSVP y acción DiffServ (pasar)

Nota: En estas combinaciones no puede existir ningún túnel manual IPSec en la misma definición de política que una acción IPSec (túnel IPSec de IKE negociado) y no se debe asociar ninguna acción RSVP con ningún tipo de

acción IPSec. Si se asocia una acción IPSec para proteger paquetes con una política, también deberá asociar una acción ISAKMP con la política.

Cada política tiene también un número de prioridad asociado (cuanto más alto es el número del atributo de prioridad, más alta es la prioridad). La prioridad determina si la política prima sobre otra política. Habitualmente, sólo se tiene que establecer si dos o más perfiles de política entran en conflicto de alguna manera. La política con un perfil más específico deberá tener una prioridad superior. Por ejemplo, suponga que una política especifica que el tráfico de la subred A a la subred B se debe proteger con IPSec (DES) y otra política especifica que el tráfico del punto a′ (un sistema principal concreto de la subred A) a la subred B se debe proteger con IPSec (3DES). La política más específica (de a′ a B) debería tener una prioridad superior a la política de A a B.

Una buena idea es designar valores de prioridad iniciales de 5 o más dígitos aparte para permitir un espacio para especificar luego valores de prioridad adicionales para las políticas que entren en conflicto. Cada política tiene también un atributo habilitado que determina si se debe habilitar cuando se carga en la base de datos de políticas. Si se encuentra una coincidencia de política durante la búsqueda en una base de datos de políticas, pero está inhabilitada, se aplica la siguiente política más específica.

Perfil

El perfil determina la información que se debe utilizar para seleccionar una política concreta. El perfil consta de información de dirección de origen, dirección de destino, protocolo y puerto de origen y de destino.

Nota: Cuando se definen políticas para IPSec/ISAKMP, cada pasarela que proporciona seguridad debe tener una política para definir la asociación de seguridad. El perfil de 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 debe encapsular en el túnel y la dirección de destino debe encontrarse en el extremo final del túnel.

También se puede seleccionar 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 de cualquier interfaz de salida se compara con los otros selectores. En algunos casos, puede tener la flexibilidad de especificar exactamente las interfaces en las que debe llegar el paquete y la interfaz en la que debe salir. Si así lo desea, debe añadir los objetos de par de interfaces y asociar el nombre de grupo de los objetos con el perfil. Puede asignar objetos de pares de interfaces a un grupo dándoles el mismo nombre. Esto le permite especificar combinaciones como (cualquier paquete que llegue a IPaddrX y salga de una interfaz *O* cualquier paquete que llegue en una interfaz y salga de IPaddrX). Esto es muy útil si define una norma de rechazo general para una interfaz pública.

Par de interfaces: Identifica la interfaz de salida y la interfaz de entrada. Especifica las direcciones IP de la interfaz para esta selección. Un valor de 255.255.255.255 incluye cualquier interfaz.

Si desea utilizar el perfil para seleccionar una política IPSec/ISAKMP, tiene la opción de especificar el ID local que se enviará durante la fase 1 y la lista de ID remotos aceptables durante las negociaciones de la fase 1. Por omisión, el ID local es el punto final de túnel local para el tráfico de IPSec/IKE y la lista de ID remota es *Any*. También puede especificar el nombre de dominio completo (FQDN), FQDN de usuario e ID de clave. Normalmente, esto es suficiente porque todas las

negociaciones de fase 1 de ISAKMP se autentican con certificados públicos o claves precompartidas. Sin embargo, en algunas situaciones de acceso remoto en las que la política es utilizar comodines para las direcciones de destino, es recomendable especificar una lista de usuarios de acceso remoto a los que se les permitirá el acceso a los recursos de la red.

Todavía se autentican estos usuarios a través de los métodos de autenticación de ISAKMP normales, pero la base de datos de políticas realiza un paso adicional al asegurar que el igual envía el ID local que coincide con uno de los ID especificados en el Grupo de usuarios remotos del perfil de la política. Es necesario si una autoridad de certificados públicos (CA) administra certificados al público general y el administrador de la red sólo quiere que un conjunto específico de estos usuarios (por ejemplo, empleados de la empresa) tenga acceso. El grupo de usuarios remotos comprende una lista de usuarios que pertenecen al mismo grupo. Estos usuarios se especifican añadiendo uno o más *USUARIOS*. Un grupo de usuarios puede crear un nombre igual como nombre de grupo para cada usuario. Este grupo también se puede asociar con un perfil.

Período de validez

El período de validez especifica la duración de la política: el año, los meses, los días y las horas en que es válida. La flexibilidad permite al administrador de la red especificar cuándo es válida una política, por ejemplo “siempre” o “sólo este año, durante los meses de enero, febrero y marzo, de lunes a viernes, de 9 AM a 5 PM.” Cuando se invalida una política de la base de datos de políticas, se aplicará la siguiente política más específica. De esta forma, puede definir una política que especifique que se proteja todo el tráfico de la subred A a la subred B de lunes a viernes de 9 am a 5 am y que en cualquier otro momento se desconecte el tráfico de la subred A a la subred B. En este caso, la primera política debe tener una prioridad superior, especificada cuando introduzca el mandato **add policy** de Talk 5).

Acción DiffServ

La acción DiffServ describe la calidad del servicio que se proporcionará a los paquetes que coinciden con una política que especifica una acción DiffServ. Puede configurar la acción DiffServ para rechazar paquetes. También puede utilizarla para correlacionar paquetes en calidades relativas de servicio. Puede configurar el ancho de banda asignado como un porcentaje de ancho de banda de salida o como un valor absoluto en Kbps. Debe especificar si la cola mejor/asegurada o la cola principal va a proporcionar la asignación de ancho de banda. Para obtener más información sobre estas colas y la manera de definirlas, consulte el Capítulo 22, “Utilización de la función de servicios diferenciados” en la página 389 y el Capítulo 23, “Configuración y supervisión de la función de servicios diferenciados” en la página 395.

La acción DiffServ también especifica cómo marcar el byte TOS antes de que se envíe a la interfaz de salida. El valor por omisión es no marcarlo. Es útil marcar los paquetes en algún punto de la red según la información de la cabecera del paquete IP. Una vez determinada la clasificación, puesto que ya se ha marcado el byte TOS, el resto de saltos de la red sólo deben mirar el byte TOS nuevo para determinar el QOS que se debe aplicar al paquete. Mirar sólo el byte TOS es mucho más eficaz y puede ser necesario para conseguir un rendimiento elevado en la red troncal DiffServ.

Acción RSVP

La RSVP especifica si se deben permitir o denegar los flujos de RSVP si se produce una reserva de RSVP y la solicitud de reserva coincide con el perfil de la política. Si desea permitir la reserva, la acción RSVP también especifica la duración permitida para la reserva, el ancho de banda y, si se quiere, una referencia a la acción DiffServ. La referencia a la acción DiffServ permite al RSVP determinar 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. El RSVP puede proporcionar el QOS hasta el límite del RSVP y luego marcar el byte TOS adecuadamente para que la red DiffServ pueda aplicar el ancho de banda correcto.

Acción IPSec

La acción IPSec puede especificar una acción de rechazo, pase o protección. Si la acción es de rechazo, todos los paquetes que coincidan con esta política se rechazarán. Si la acción es de pase sin seguridad, se autoriza el pase a todos los paquetes. Si la acción es de pase con seguridad, todos los paquetes se protegen a través de la asociación de seguridad (SA) especificada por la acción. La acción IPSec también contiene las direcciones IP de los puntos finales del túnel para el túnel IPSec y los SA de IKE.

Las propuestas de IPSec a las que hace referencia la acción IPSec determinan los atributos de SA. La acción IPSec puede especificar varias propuestas de IPSec que se envían y comprueban en el orden en que se han especificado. Si se tienen diversas propuestas en una acción IPSec, se permite a la configuración contener todas las combinaciones de seguridad aceptables, por lo que se reduce el número de no coincidencias de configuración potenciales entre pasarelas VPN.

Propuesta de IPSec

La propuesta de IPSec contiene la información acerca de la transformación de ESP, AH, (o ambos) que se propone o comprueba durante las negociaciones de ISAKMP de la fase 2. Si necesita un reenvío secreto perfecto (un cálculo Diffie Hellman nuevo), la propuesta de IPSec identifica el grupo DH que se debe utilizar. Las transformaciones a las que hace referencia la propuesta de IPSec se envían o comprueban en el orden en que se han especificado. La primera transformación de ESP o AH de la lista debe ser la más apropiada. Si hay más de una en la lista, cada una se compara con la lista de transformaciones de iguales para encontrar una coincidencia. Si ninguna de las transformaciones configuradas coinciden con la lista de iguales, la negociación falla. La propuesta de IPSec puede listar una combinación de transformaciones de AH y ESP, pero las únicas combinaciones válidas son:

- Lista sólo de AH (modalidad de túnel o transporte)
- Lista sólo de ESP (modalidad de túnel o 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 del cifrado de IPSec y los parámetros de autenticación y especifican también la frecuencia de renovación de las claves. La transformación es AH (sólo autenticación) o ESP (cifrado, autenticación o ambas) y se puede configurar para que funcione en modalidad de túnel o de transporte.

Acción ISAKMP

La acción ISAKMP especifica la información de gestión de claves para la fase 1. Especifica si las negociaciones de la 1 deben empezar en modalidad principal (proporciona protección de identidad) o en modalidad agresiva. También especifica si la asociación de seguridad de la fase 1 se debe negociar al iniciar el dispositivo o bajo petición. La acción ISAKMP también debe hacer referencia a una o más propuestas de ISAKMP. La primera referencia debe ser para la propuesta de ISAKMP 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 el grupo de Diffie Hellman que se debe utilizar para generar las claves y la duración de la asociación de seguridad de la fase 1. Debe seleccionar el método de autenticación en la propuesta de ISAKMP. Puede ser una modalidad de certificados o una clave precompartida.

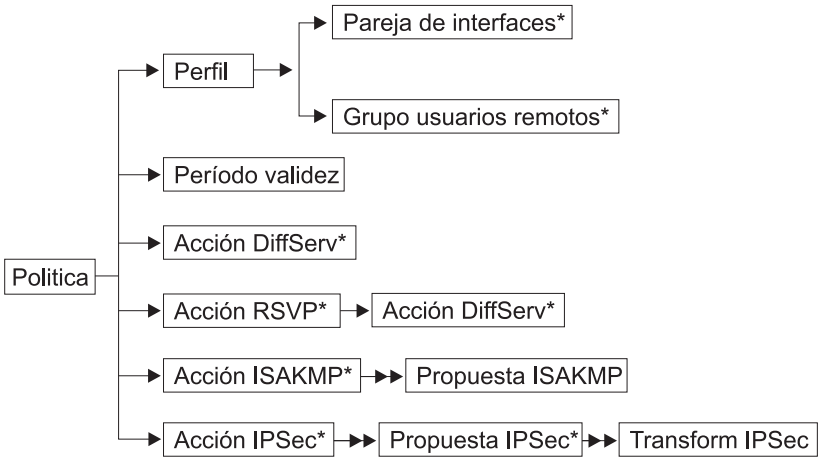
Usuario

Debe configurar un USUARIO para cualquier política que utilice una negociación de ISAKMP con clave precompartida como método de autenticación. La configuración de USUARIO identifica la clave precompartida que se debe utilizar para el igual ISAKMP. El objeto de usuario contiene la información de identificación para un igual ISAKMP remoto, es decir la dirección IP, FQDN, ID de clave o FQDN de usuario y el método que el usuario quiere utilizar para la autenticación. Puede seleccionar una modalidad de certificados o una clave precompartida. Si selecciona la clave precompartida, también debe especificar si se debe introducir en ASCII o hexadecimales y el valor de la clave. Los USUARIOS se pueden agrupar asignándolos al mismo nombre de grupo. Este grupo también se puede asociar con un perfil de políticas para llevar a cabo una búsqueda de política más estricta para la fase 1.

Túnel con claves manuales IPSec

El túnel con claves manuales IPSec es una configuración estática de los parámetros de cifrado y autenticación. No se realiza ninguna negociación para el túnel, de manera que los dos iguales deben tener exactamente la misma configuración. Las claves se introducen como parte de esta configuración y deben coincidir en ambos lados del túnel. Puesto que no se realiza ninguna negociación en esta modalidad, las claves no se renuevan nunca. Para obtener más información sobre los túneles con claves manuales IPSec, consulte la descripción de la función IPSec en el Capítulo 20, “Utilización de la seguridad IP” en la página 335.

La Figura 27 en la página 283 muestra la relación entre los objetos de configuración de una política.



Notas:

1. La flecha → indica una referencia simple.
2. La flecha →→ indica una referencia múltiple.
3. El * indica una referencia opcional.
4. En una política de seguridad para ISAKMP/IPSec, el perfil de tráfico define el tráfico que pasa al túnel seguro.

Figura 27. Relación de los objetos de configuración de una política

Interacción de la base de datos de políticas y LDAP

La familia de direccionadores permite que un servidor LDAP (Lightweight Directory Access Protocol) sea el depósito de información de la política (la base de datos de políticas). El LDAP es un protocolo que permite la búsqueda y modificación en un servidor de directorios. El LDAP es una versión sencilla del estándar X.500. Los direccionadores dan soporte a la posibilidad de búsqueda (pero no de modificación) de información en el servidor de directorios. El agente de búsqueda de la política del direccionador recupera toda la información del servidor de directorios que se refiere a ese dispositivo. Todos los servidores LDAP que funcionan en el LDAP versión 2 o 3 funcionan con la implementación en el direccionador. Una ventaja importante de la utilización de un servidor de directorios para almacenar información de política, en comparación con los métodos más tradicionales de configuración almacenada localmente, es la posibilidad de realizar un cambio en un lugar y que ese cambio se aplique a todos los dispositivos de la red ampliada. Esto incluye los dispositivos del dominio administrativo, así como los dispositivos a través de los límites públicos.

Por ejemplo, suponga que tiene una definición de transformación de IPSec que reside en el directorio. Si quiere cambiar la política corporativa para el cifrado de DES a 3DES, normalmente deberá realizar un cambio en cada configuración de dispositivo que se encuentra en cada límite de la red. Si utiliza el directorio para desplegar las políticas, sólo deberá cambiar una transformación de IPSec. Después cada uno de los dispositivos habilitados para políticas de la red deberá volver a crear la base de datos. Otro ejemplo: suponga que tiene que cambiar una acción DiffServ denominada “GoldService” para aumentar el valor de ancho de banda del 40% al 45%. El servidor LDAP y la infraestructura de la política permite que los tipos de cambios de la configuración se ajuste mejor proporcionalmente y reduce las no coincidencias en la configuración.

Utilización de la función de política

Si es el administrador de la red, también puede aprovechar la posibilidad de renovar la base de datos automáticamente a una hora especificada cada día. Para seleccionar esta opción, entre el mandato **set refresh** de la opción de política. También puede especificar si quiere habilitar la renovación y, si se habilita, la hora en que desea que se renueve la base de datos. Esta opción es útil para efectuar cambios automatizados. Por ejemplo, suponga que debe añadir una política nueva para que el departamento de márketing de EE.UU. pueda hablar con el departamento de desarrollo de Japón a través de Internet y que las pasarelas de seguridad son SG1 y SG2. Sólo tiene que entrar esta información en el directorio y, a medianoche, las pasarelas SG1 y SG2 efectuarán automáticamente este cambio si tienen habilitada la renovación automática.

El motor de búsqueda de políticas LDAP le permite especificar el nivel de seguridad que se utilizará al crear la base de datos de políticas. Estas opciones de seguridad se definen con el mandato **set default** de funciones de política. Las opciones son:

- Pasar todo el tráfico durante la búsqueda (valor por omisión).
- Desconectar todo el tráfico *excepto* las solicitudes de búsqueda de políticas de LDAP y los resultados.
- Desconectar todo el tráfico *excepto* las solicitudes de búsqueda de políticas de LDAP y los resultados protegidos por IPSec.

En algunas situaciones, una de las dos primeras opciones es suficiente. Sin embargo, si el tráfico del LDAP tiene que atravesar la infraestructura pública, debería proteger y autenticar la información seleccionando la tercera opción. Si lo hace, debe seleccionar las opciones de cifrado y autenticación de las fases 1 y 2. También debe entrar las direcciones IP para los puntos finales del túnel (servidores LDAP principal y secundario). Este túnel IKE/IPSec de rutina de carga se negociará antes de que se envíe el tráfico de LDAP. Esta función le permite establecer la configuración que aparece en la Figura 28.

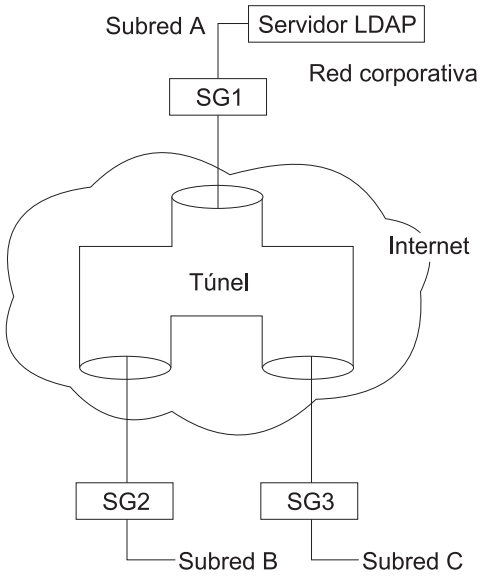


Figura 28. Protección del tráfico a través de Internet

Esta figura muestra un servidor LDAP de la Subred A de la red corporativa. SG1, SG2 y SG3 buscan sus políticas en el servidor LDAP. La búsqueda de políticas para SG2 y SG3 se produce a través de Internet y está protegida mediante IPSec.

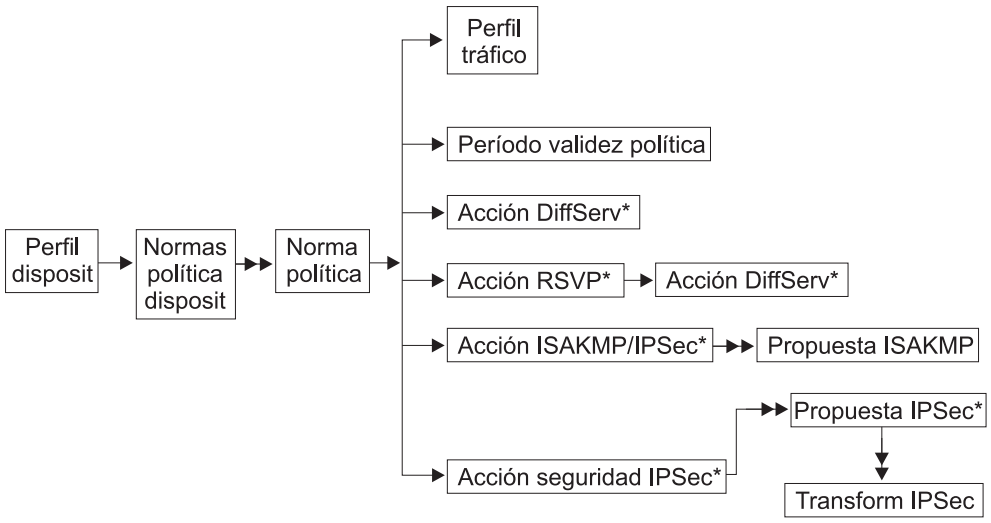
La información de configuración necesaria para la base de datos de políticas para recuperar satisfactoriamente las políticas del directorio es:

- Dirección IP del servidor principal (también se puede configurar un servidor secundario de copia de seguridad)
- Número de puerto en el que el servidor escucha (nota: no se da soporte a SSL y TLS)
- La información de nombre de usuario y contraseña es obligatoria
- Nombre distintivo base del objeto DeviceProfile para este direccionador o clase de direccionadores.
- Información de política por omisión

Cuando haya introducido esta información de configuración, la próxima vez que se renueve la base de datos de políticas se intentará pedir la información de política al servidor de directorios. la base de datos de políticas permite una combinación de políticas configuradas localmente y normas leídas del servidor LDAP. Si se encuentran dos normas que entran en conflicto y tienen la misma prioridad, la norma leída en la configuración local prima sobre la norma leída en el servidor de directorios.

Esquema de política

El esquema de LDAP es el conjunto de normas e información que conforman las definiciones de clase y atributo que determinan el contenido de las entradas del directorio. Generalmente, el esquema de LDAP se graba en una sintaxis de ASN1, similar a los MIB del SNMP. El esquema de política al que da soporte esta familia de direccionadores es un trabajo que comprende esfuerzos de pre-estándar que se realiza en el IETF. Se basa en el trabajo de seguimiento de estándares realizado por el IPSec y los Grupos de trabajo de políticas del IETF y el del DMTF. El esquema de política coincide en gran manera con los objetos de configuración existentes en la función de política del direccionador. Puede encontrar los archivos de definición del esquema de política y los del servidor LDAP si accede a la URL: **http://www.networking.ibm.com/support**. Seleccione el producto de direccionador que desee y seleccione el enlace *Downloads*. La Figura 29 en la página 286 muestra la estructura global del esquema de política.



Notes:

1. La flecha → indica una referencia simple.
2. La flecha →► indica una referencia múltiple.
3. El * indica una referencia opcional.
4. En una política de seguridad para ISAKMP/IPSec, el perfil de tráfico define el tráfico que pasa al túnel seguro.

Figura 29. Estructura del esquema de política

DeviceProfile y DevicePolicyRules son dos objetos clave en el esquema de política. Habilitan el agente de búsqueda de políticas para localizar las políticas necesarias para el dispositivo. El DeviceProfile contiene información acerca de la dirección IP administrativa del dispositivo y una referencia a DevicePolicyRules preceptiva. Puede agrupar los dispositivos en un DeviceProfile o cada dispositivo de la red puede tener su propio DeviceProfile. La opción que elija dependerá de si hay más de un dispositivo en la red que deba buscar el mismo conjunto de normas. Esto no suele ser así para las pasarelas de seguridad, puesto que todas tienen un punto final de túnel distinto. Para los dispositivos que no son de QOS, es probable que todos los dispositivos de un grupo lean el mismo conjunto de políticas.

El objeto DevicePolicyRules se recupera según el valor del DeviceProfile que se busca para el dispositivo. Una vez recuperado el objeto DevicePolicyRules, se puede recuperar la lista de PolicyRules. Si no se encuentra un objeto o si se detecta un error durante la comprobación de coherencia en un objeto, se cancela la búsqueda y se visualizan los mensajes en ELS (mensajes PLCY) que identifican el error. Si se produce un error, el administrador de la red puede configurar una de las siguientes opciones para manejarlas:

- Suprimir todas las políticas leídas localmente e invertir a un rechazo o pase toda la norma
- Mantener todas las políticas leídas localmente. Especifique esta opción con el mandato **set default** de la función de política.

En cualquier caso, se intenta la búsqueda en el intervalo de reintentos configurado. Si no se puede conectar con el servidor LDAP principal, se intenta con el servidor secundario después de 5 intentos. Si no se puede conectar con el servidor secundario, se vuelve a intentar con el servidor principal después de 5 intentos. Puede especificar el intervalo de reintentos con el mandato **set ldap retry-interval**

de la función de política. Si falla una búsqueda debido a la latencia de la red, puede cambiar el tiempo de espera de búsqueda del valor por omisión de 3 segundos mediante el mandato **set ldap search-timeout** de la función de la política.

Generación de normas

Configure una política para especificar cómo quiere que funcione la red. El direccionador convierte la información de política en un conjunto de normas que compara con los flujos de tráfico. Antes, esto se hacía de forma manual definiendo los filtros de paquetes de entrada y salida para cada patrón de tráfico. La base de datos de políticas lo elimina, porque sólo deberá configurar una sola política.

La mayor parte del trabajo se realiza de forma interna cada vez que se construye la base de datos de políticas. En algunos casos, un direccionador convierte una política directamente en una sola norma. En el caso de ISAKMP/IPSec, convierte una política en cinco normas. Son necesarias cinco normas para dar cuenta de las direcciones del tráfico (entrada y salida) y para los flujos de control que se producen durante las negociaciones de IKE de las fases 1 y 2. La relación entre políticas y normas es la siguiente:

Una política DiffServ → Una norma DiffServ

Una política RSVP → Una norma RSVP

Una política ISAKMP/IPSec → Cinco normas ISAKMP/IPSec

Ejemplo: Proteja el tráfico de la subred A a la subred B; los puntos finales del túnel son SGa y SGb

1. Entrada de fase 1 (Profile = SGb to SGa, Proto UDP, Src Port 500, Dst Port 500): Esta norma es necesaria para filtrar las negociaciones de fase 1 de entrada del igual ISAKMP remoto si el dispositivo funciona como responder ISAKMP.
2. Salida de fase 1 (Profile = SGa to SGb, Proto UDP, Src Port 500, Dst Port 500): Esta norma es necesaria para filtrar la información de fase 1 necesaria si el tráfico inicia las negociaciones de fase 1 de ISAKMP. En este caso, el dispositivo funciona como iniciador de ISAKMP.
3. Entrada de fase 2 (Profile = SGb to SGa, Proto UDP, Src Port 500, Dst Port 500): Esta norma es necesaria para filtrar el tráfico de fase 2 de entrada del igual ISAKMP remoto. Este tráfico es el resultado del igual remoto que inicia una negociación inicial o renovación de fase 2. No es necesaria ninguna norma de salida de fase 2, puesto que el tráfico de salida (norma 5) siempre inicia las negociaciones si hace falta.
4. Tráfico hacia el túnel protegido (Profile = Subnet A to Subnet B): Esta norma es necesaria para colocar el tráfico no protegido en un túnel de seguridad. Si no se ha negociado la asociación de seguridad, se recopila también la norma de fase 1 e IKE inicia las fases 1 y 2. Cuando se han establecido los SA, los paquetes que coinciden con esta norma se entregan a IPSec para la encapsulación y transmisión.
5. Tráfico del túnel protegido (Profile = Subnet B to Subnet A): Esta norma es necesaria para asegurar que los paquetes que deberían haber llegado en un túnel protegido han llegado realmente en éste. Si el IPSec no ha

desencapsulado el paquete y encuentra esta norma, se rechaza el paquete. Esta norma maneja el tráfico que se cuela en la red.

Un túnel IPSec con claves manuales → Dos normas IPSec

Ejemplo: Proteja el tráfico de la subred A a la subred B; los puntos finales del túnel son SGa y SGb.

1. Tráfico hacia el túnel protegido (Profile = Subnet A to Subnet B): Esta norma es necesaria para colocar el tráfico no protegido en un túnel de seguridad. Es un túnel configurado estáticamente para que esté siempre disponible y los paquetes que coinciden con esta norma se dirigen directamente a IPSec para la encapsulación y transmisión.
2. Tráfico del túnel protegido (Profile = Subnet B to Subnet A): Esta norma es necesaria para asegurar que los paquetes que deberían haber llegado en un túnel protegido han llegado realmente en éste. Si el IPSec no ha desencapsulado el paquete y encuentra esta norma, se rechaza el paquete. Esta norma maneja el tráfico que se cuela en la red.

Puede ver estas normas con el mandato **list rule** de Talk 5 de la función de política.

Ejemplos de configuración

Los siguientes ejemplos muestran cómo utilizar la función de política para configurar los direccionadores de una red. Primero, acceda a la función de política::

```
* talk 6
Config>feature policy
IP Network Policy configuration
```

Política IPSec/ISAKMP con QOS

Puede entrar la información de política de dos formas distintas. La primera es definir los objetos de política individuales y agruparlos después. Para utilizar este método, defina primero las transformaciones de IPSec y luego la propuesta de IPSec (que se refiere a las transformaciones de IPSec). Luego defina la acción IPSec (que se refiere a propuesta de IPSec) y así sucesivamente hasta que haya definido completamente la política. Con la Figura 30 en la página 289 como referencia, este método se inicia a la derecha de los objetos de política y funciona hasta la izquierda.

La segunda posibilidad, que es más fácil, es definir primero las opciones de política de un nivel superior y, según se le indique, entrar las definiciones para los objetos de política individuales según corresponda. Después de la Figura 30 en la página 289 se incluye un ejemplo de procedimiento de configuración que utiliza los valores que corresponden a los de la figura. Utiliza el método de izquierda a derecha y se inicia con el mandato **add policy**.

Si ha definido anteriormente un objeto que cumpla sus necesidades, puede volver a utilizarlo en vez de crear una definición nueva. Por ejemplo, si se ha configurado un período de validez para allTheTime para una política anterior, puede utilizarlo. El siguiente procedimiento muestra todo el proceso, pero no muestra la reutilización de la información de política definida anteriormente. Para ver un

ejemplo del uso de la información definida anteriormente, consulte el apartado "Política de sólo IPSec/ISAKMP" en la página 300.

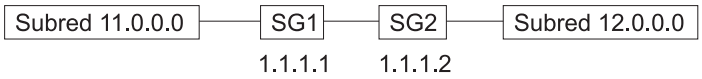


Figura 30. Configuración de IPSec/ISAKMP con QOS

El marco hipotético de configuración de política descrito en el siguiente texto es desde la perspectiva de SG1. La sentencia de política es:

Proteja el tráfico de la subred 11 a la subred 12 con los puntos finales del túnel SG1 y SG2, y proporcione un QOS para el tráfico de 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. Definición de perfil nuevo; en este caso el tráfico que nos interesa es el de la subred 11 a la subred 12.

```
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 del perfil y vuelto al menú de configuración de la 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. Cuestiones de configuración del período de validez; en este ejemplo el período de validez es de 9 AM a 5 PM, de lunes a viernes, 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:
  yyyymmddhhmmss:yyyymmddhhmmss 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 vuelto al menú de configuración de la 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. Defina siempre una acción IPSec nueva porque el punto final del túnel será siempre distinto. Las excepciones son si hay varios túneles entre las dos pasarelas, y en las configuraciones de acceso remoto con comodines donde el punto final del túnel es desconocido.

```
IPSEC Actions:
 0: New IPSEC Action

Enter the Number of the IPSEC Action [0]?
```

9. Menú de acción IPSec.

```
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 configurada, por lo que debe definir una nueva. Tenga en cuenta que cuando se haya definido la propuesta de IPSec, se puede volver a utilizar en las múltiples acciones IPSec.

```
List of IPSEC Proposals:
 0: New Proposal

Enter the Number of the IPSEC Proposal [0]?
```

11. Configure 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. Cuando haya definido la transformación de ESP, cualquier propuesta de IPSec puede volver a utilizarla.

```
List of ESP Transforms:
 0: New Transform

Enter the Number of the ESP transform [0]? 0
```

13. Configure la transformación de IPSec.

```
Enter a Name (1-29 characters) for this IPsec Transform []? esp3DESwSHA
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  = esp3DESwSHA
 Type =ESP   Mode =Tunnel     LifeSize=   50000 LifeTime=    3600
 Auth =SHA   Encr =3DES
Is this correct? [Yes]:
```

14. Vuelva al menú de propuesta de IPSec.

```
List of ESP Transforms:
 0: New Transform
 1: esp3DESwSHA

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:
  esp3DESwSHA
Is this correct? [Yes]:
```

15. Vuelva al menú de acción IPSec.

```
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. Vuelva 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 IPSec protegida, por lo que debe identificar una acción ISAKMP para las negociaciones de la fase 1. No hay ninguno definido, debe entrar uno nuevo. En la mayoría de los casos, son suficientes una propuesta y una acción ISAKMP para todas las políticas de seguridad.

```
ISAKMP Actions:
 0: New ISAKMP Action

Enter the Number of the ISAKMP Action [0]?
```

18. Configure la acción 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 lifesize/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 ISAKMP configurada, por lo debe crear una nueva.

```
List of ISAKMP Proposals:
 0: New Proposal
```

20. Configure la propuesta de ISAKMP.

```
Enter the Number of the ISAKMP Proposal [0]?
Enter a Name (1-29 characters) for this ISAKMP Proposal []? genP1Proposal

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 = genP1Proposal
 AuthMethod = Pre-Shared Key
 LifeSize   = 1000
 LifeTime   = 15000
 DHGroupID  = 1
 Hash Algo  = SHA
 Encr Algo  = 3DES CB
Is this correct? [Yes]:
```

21. Vuelva a la configuración de acción ISAKMP.

```
List of ISAKMP Proposals:
 0: New Proposal
 1: genP1Proposal

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:
  genP1Proposal
Is this correct? [Yes]:
```

22. Vuelva a la configuración de la política.

```
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]: yes
```

23. Defina la acción DiffServ GoldService.

```
DiffServ Actions:
 0: New DiffServ Action

Enter the Number of the DiffServ Action [0]?
```

24. Configure la acción DiffServ.

```
Enter a Name (1-29 characters) for this DiffServ Action []? GoldService
Enter the permission level for packets matching this DiffServ
Action (1. Permit, 2. Deny) [2]? 1
List of DiffServ Queues:
   1) Premium
   2) Assured/BE
Enter the Queue Number(1-2) for outgoing packets matching
this DiffServ Action [2]? 2
How do you want to specify the bandwidth allocated to this service?
Enter absolute kbps(1) or percentage of output bandwidth(2) [2]?
Enter the percentage of output bandwidth allocated to this service [10]? 40

Transmitted DS-byte mask [0]?
Transmitted DS-byte modify value [0]?

Here is the DiffServ Action you specified...

DiffServ Name   = GoldService                    Type =Permit

 TOS mask:modify=x00:x00
 Queue:BwShare  =Assured    : 40 %
Is this correct? [Yes]:
```

25. Vuelva a la configuración de la política.

```
DiffServ Actions:
 0: New DiffServ Action
 1: GoldService

Enter the Number of the DiffServ Action [1]? 1
Policy Enabled/Disabled (1. Enabled, 2. Disabled) [1]?

Here is the Policy you specified...

Policy Name     = examplePolicySecure11to12
 State:Priority =Enabled    : 10
 Profile        =trafficFrom10NetTo12Net
 Valid Period   =MonToFri-9am:5pm-1999
 IPSEC Action   =secure11NetTo12Net
 ISAKMP Action  =genPhase1Action
 DiffServ Action=GoldService
Is this correct? [Yes]:
```

26. Si no se han habilitado DiffServ o IPSec, se le advierte que antes de que se aplique la política, debe habilitar DiffServ, IPSec o ambos (la función DiffServ o IPSec).

```
You must enable and configure DiffServ in feature DS before
QOS can be ensured for this policy
```

27. El paso final de este proceso es añadir una definición de perfil de USUARIO para el igual ISAKMP remoto. Este paso no es necesario si las negociaciones ISAKMP deben autenticar el igual con certificados públicos. Sin embargo, en el ejemplo anterior hemos elegido la clave precompartida como método de autenticación y deberá identificar el usuario y entrar la clave precompartida que esperamos que utilice el par.

```
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. Los pasos de configuración han finalizado. Si desea configurar DiffServ, IPSec, o cualquier red o configuración de IP, debe hacerlo antes de que el túnel IPSec funcione. El siguiente ejemplo de mandato de lista muestra la configuración que se ha completado. Para activar estos cambios, vuelva a cargar el dispositivo o entre el mandato **reset database** de Talk 5 de la función 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:
  esp3DESwSHA
--More--

Configured IPSEC Transforms....
```

```
Transform Name  = esp3DESwSHA
 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 de sólo IPSec/ISAKMP

Un ejemplo de procedimiento de configuración, que sigue a la Figura 31 y utiliza valores que corresponden a los de la figura, utiliza el método de izquierda a derecha y muestra cómo crear sobre el ejemplo de procedimiento anterior volviendo a utilizar la información que ha creado la anterior.

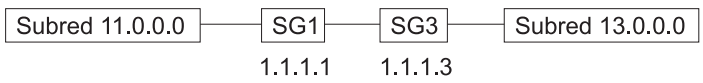


Figura 31. Configuración de IPSec y utilización de una definición anterior

El marco hipotético de configuración de política descrito en el siguiente texto es desde la perspectiva de SG1. La sentencia de política en este marco es:

Proteja el tráfico de la subred 11 a la subred 13 (sólo tráfico de TCP) con los puntos finales del túnel SG1 y SG3, y no proporcione ningún QOS.

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.

```
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 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]:
```

Desconexión de todo el tráfico público (norma de filtro)

Este ejemplo de política muestra cómo configurar una norma de desconexión sencilla para la interfaz pública que desconecta todo el tráfico que no está protegido mediante el IPSec. Esta norma es muy general y **debe** tener la prioridad inferior a todas las normas 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 de entrada o salida 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. Puesto que la información de origen o destino (o ambas) se han separado con un comodín, debe especificar las interfaces de las que espera que llegue y salga el tráfico.

```
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 un par de interfaces para el tráfico que sale a través de la interfaz pública.

```
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 otro par de interfaces para el tráfico que entra a través de la interfaz pública. Déle el mismo nombre que al par de interfaces anterior para asignarlo 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 período de validez que especifique `all the time`.

```
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 acción IPSec nueva para desconectar todo el tráfico (acción de filtro).

```
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 políticas LDAP

Este ejemplo muestra cómo configurar y habilitar el motor de búsqueda de políticas LDAP En este ejemplo hay dos directorios LDAP (uno principal y uno secundario) con direcciones IP de 11.0.0.2 y 13.0.0.1 respectivamente. Los dos escuchan en el puerto 389 de TCP y el dispositivo debe enlazarse con el servidor LDAP como cn=router, password miContraseña. La entrada base en el árbol del directorio para las políticas del direccionador es cn=RouterDeviceProfile,o=ibm,c=us.

Nota: Actualmente, los servidores LDA primario y secundario deben escuchar el mismo puerto y tener las mismas credenciales de autenticación para el direccionador. El DeviceProfile debe ser el mismo para el direccionador de los dos servidores de directorios.

Este ejemplo muestra también cómo establecer la política por omisión para que las comunicaciones de LDAP estén protegidas a través del IPSec. Este ejemplo utiliza una clave precompartida para la autenticación de ISAKMP, y SHA y 3DES para los parámetros de autenticación y cifrado para las fases 1 y 2. El punto de inicio del túnel es 1.1.1.4 para el dispositivo que lleva a cabo la búsqueda de políticas de 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 políticas 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. Establezca la política por omisión

```
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 este momento, está listo para gestionar los direccionadores de la red con la función de política. Para obtener información detallada sobre los mandatos utilizados para configurar los parámetros de política necesarios como perfiles, propuestas, transformaciones y acciones, consulte los apartados “Mandatos de configuración de la política” en la página 311, “Mandatos de configuración del servidor de políticas de LDAP” en la página 325 y “Mandatos de supervisión de la política” en la página 329.

Capítulo 19. Configuración y supervisión de la función de política

Este capítulo describe los mandatos de política y LDAP proporcionados por la función de política para configurar y utilizar los dispositivos de direccionador de una red. Incluye los siguientes apartados:

- "Acceso al indicador de configuración de la política"
- "Mandatos de configuración de la política"
- "Mandatos de configuración del servidor de políticas de LDAP" en la página 325
- "Acceso al indicador de supervisión de la política" en la página 329
- "Mandatos de supervisión de la política" en la página 329

Acceso al indicador de configuración de la política

Para entrar los mandatos de configuración de la política:

1. Entre **talk 6** en el indicador OPCON (*).
2. Entre **feature policy** en el indicador Config>.

Aparecerá el indicador Policy config>. Ahora puede entrar los mandatos de configuración de la política.

Mandatos de configuración de la política

Estos mandatos le permiten configurar la información contenida en las políticas. La Tabla 38 resume los mandatos de configuración de la política y el resto de este apartado los describe detalladamente. Escriba estos mandatos en el indicador Policy config>. Puede entrar el mandato y las opciones en una línea o entrar sólo el mandato y responder a las indicaciones. Para ver una lista de opciones de mandato válidas, entre el mandato con un interrogante en vez de las opciones.

Tabla 38. Mandatos de configuración de la política

Mandato	Función
? (Ayuda)	Visualiza todos los mandatos disponibles para este nivel de mandato, o lista las opciones de mandatos específicos (si es que están disponibles). Consulte "Obtención de ayuda" en la página xxv.
Add	Añade la información utilizada para crear una política.
Change	Cambia la información que constituye 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	Muestra la información de una política.
Set	Especifica una política que se utilizará como valor por omisión.
Exit	Hace volver al nivel de mandato anterior. Consulte "Salida de un entorno de nivel inferior" en la página xxv.

Add

Utilice el mandato **add** para añadir información en 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
Le solicita información acerca de las selecciones de DiffServ-action que se deben aplicar.

Name
El nombre exclusivo de la acción DiffServ para la política.

permission-level
Especifica si el direccionador debe reenviar los paquetes que coincidan con esta acción DiffServ.

1 Permitir

2 Denegar

Valor por omisión: 2

Queue-priority
La cola donde se colocan los paquetes de salida que coinciden con esta acción DiffServ.

1 Principal (reenvío activado)

2 Asegurado / mejor

Valor por omisión: 2

bwshare-type
El tipo de asignación de compartimento de ancho de banda.

1 Absoluto (en Kbps)

2 Porcentaje (del total de ancho de banda de salida)

Valor por omisión: 2

bwshare
El ancho de banda (en Kbps o como porcentaje del ancho de banda de salida) asignado a este servicio.

ds-bytemask
La máscara que se debe aplicar a los bytes de ds transmitidos. Este valor designa los bits del byte TOS de un paquete que se debe cambiar cuando se transmite el paquete. Un cero en cualquier posición de bit de este byte implica que el bit no se debe cambiar.

Valor por omisión:

00

(no cambiar ningún bit)

ds-bytemodify
La marca del byte TOS de IP que se debe aplicar a los paquetes que reenviará este dispositivo. Los ceros de la máscara implican que el bit correspondiente no se cambiará. Un uno implica que el bit se marcará con el valor de bit del byte de marca. La operación es: newTOSByte = (Mask & receivedTOSByte) | (Mask&Mark) El ^ ∧ es un complemento basado en bits (Mask:Mark)

Ejemplo:

```
11111101:00000001
```

En este ejemplo, un valor recibido de 0x07 se enviaría con un valor de 0x03

Valor por omisión: X'00' (no cambiar ningún bit)

interface-pair
El par de interfaces asocia un perfil con una interfaz específica o un conjunto de interfaces. Por omisión, el objeto de perfil no restringe la aplicación de 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 de la que debe salir el tráfico.

El ejemplo siguiente muestra dos pares de interfaces con el mismo nombre que representan el tráfico que entra en cualquier interfaz y sale de la interfaz pública y a la inversa.

```
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
El nombre del par de interfaces.

Ingress interface
Dirección IPv4 de la interfaz de entrada.

Valor por omisión: 255.255.255.255 (any)

Egress interface
Dirección IPv4 de la interfaz de salida.

Valor por omisión: 255.255.255.255 (any)

IPSec-action
Le solicita información para configurar el túnel de fase 2.

Name
El nombre de la acción IPSec.

Action type
La acción que se aplicará a los paquetes que coincidan con el perfil de una política que contenga esta acción.

1 Bloquear (bloquear conexión).

2 Permitir (permitir los paquetes que coincidan con esta acción). Si no existe ninguna propuesta de IPSec, pasar el paquete; si existe una propuesta de IPSec, aplicar el proceso de seguridad IPSec en el paquete.

Valor por omisión: 2

La siguiente opción sólo está disponible si especifica pasar como tipo de acción:

Traffic flow type
Tipo de flujo de tráfico (túnel protegido o libre).

1 Libre

2 Túnel protegido

Valor por omisión: 2

La siguiente opción sólo está disponible si especifica el flujo de tráfico en protegido:

Tunnel start point
Dirección IPv4 del punto de inicio 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 protegerlo también otra política configurada en este dispositivo.

Opciones válidas: Yes o No

Valor por omisión: No

Percentage of SA lifesize/lifetime to accept
Duración mínima de la SA (como porcentaje) de la duración de la SA. No se aceptará una duración con un valor inferior a éste.

Valor por omisión: 75

SA refresh threshold
El porcentaje en la duración de la SA o el valor de duración en que se debe renovar automáticamente la SA.

Valor por omisión: 85

DF-Bit-Setting
Especifica si se debe copiar el bit de no fragmentación del paquete original y si se debe establecer o borrar en la cabecera exterior del paquete de IPSec si se ejecuta en modalidad de túnel.

1 Copiar

2 Establecer

3 Borrar

Valor por omisión: 1

Replay-Prevention
Especifica si el IPSec debe aplicar la prevención de repetición para los paquetes de IPSec recibidos. En esta modalidad, el 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 el SA de la 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 hasta cinco propuestas) que se enviará o comprobará durante la fase 2. El orden en que se especifiquen determinará su prioridad: la primera será la superior.

IPSec-manual-tunn
Le solicita información para configurar manualmente el túnel de fase 2.

Tunnel name
El nombre del túnel manual de IPSec.

Tunnel lifetime
La duración del túnel (en minutos).

Valor por omisión: 46080

Encapsulation mode
La modalidad de encapsulación que se utilizará.

tunn
Modalidad del túnel

trans
Modalidad de transporte

Valor por omisión: tunn

Policy
El tipo de política de túnel que se utilizará.

AH
Cabecera de autenticación

ESP
Carga útil de seguridad de encapsulación

AH-ESP
Para los paquetes de salida, especifica que el cifrado se ejecuta antes que la autenticación.

ESP-AH
Para los paquetes de salida, especifica que la autenticación se ejecuta antes que el cifrado.

Valor por omisión: AH-ESP

Local IP address
La dirección IPv4 de origen.

Valor por omisión: 11.0.0.5

Local encryption SPI
El valor de índice de los parámetros de seguridad de origen.

Valor por omisión: 256

Local encryption algorithm
El algoritmo de cifrado de origen.

Null
Sin cifrado.

CDMF
Commercial Data Masking Facility.

DES-CBC
Data Encryption Standard and Cipher Block Chaining.

3DES
Triple Data Encryption Standard.

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 va a utilizar la autenticación de ESP local.

Yes o No

Valor por omisión: Yes

Remote IP address
La dirección IPv4 de destino.

Valor por omisión: 0.0.0.0

Remote encryption SPI
El valor de índice de los 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.

DES-CBC
Data Encryption Standard and Cipher Block Chaining.

3DES
Triple Data Encryption Standard.

Valor por omisión: DES-CBC

Remote encryption key
Una clave de 16 caracteres.

Verify remote encryption padding.
Especifica si se verificará el relleno de cifrado remota.

Yes o No

Valor por omisión: No

Remote ESP authentication
Especifica si se va a utilizar la autenticación de ESP remota.

Yes o No

Valor por omisión: Yes

DF bit
Especifica cómo se debe procesar el bit de no fragmentación.

Copy
Copia el bit DF.

Set
Activa el bit DF.

Clear
Desactiva el bit DF.

Valor por omisión: COPY

Enable tunnel
Especifica si se debe habilitar el túnel cuando se cree.

Yes o No

Valor por omisión: Yes

IPSec-proposal
Le solicita información para la creación de una propuesta de IPSec.

IPSec proposal name
El nombre de la propuesta de IPSec.

Perfect forward secrecy
Especifica si se va a utilizar el IKE, para evitar que cualquiera determine una clave actual desde una clave concedida anteriormente.

Yes o No

Valor por omisión: No

Diffie Hellman Group ID
El tipo de grupo Diffie Hellman.

1 Diffie Hellman Grupo 1

2 Diffie Hellman Grupo 2

Valor por omisión: 1

AH transform
El nombre de la transformación de AH (puede especificar hasta cinco transformaciones) para esta propuesta. El orden en que se especifiquen determinará su prioridad: la primera será la superior.

ESP transform
El nombre de la transformación de ESP (puede especificar hasta cinco propuestas) para esta propuesta. El orden en que se especifiquen determinará su prioridad: la primera será la superior.

IPSec-transform
Le solicita información acerca de las transformaciones de IPSec.

IPSec transform name
El nombre de la transformación de IPSec.

Protocol ID
El protocolo de seguridad que se utilizará.

1 IPSec-AH

2 IPSec-ESP

Valor por omisión: 1

AH Authentication Algorithm
El algoritmo de autenticación de AH que se utilizará.

1 HMAC-MD5

2 HMAC-SHA

Valor por omisión: 1

Encapsulation mode
La modalidad de encapsulación que se utilizará.

1 Túnel

2 Transporte

Valor por omisión: 1

ESP Authentication Algorithm
El algoritmo de autenticación de ESP que se utilizará.

0 Ninguno

1 HMAC-MD5

2 HMAC-SHA

Valor por omisión: 2

ESP cipher algorithm
El algoritmo de cifras de ESP que se utilizará.

1 ESP DES

2 ESP 3DES

3 ESP CDMF

4 ESP Null (sin cifrado)

Valor por omisión: 1

SA lifesize
La duración (en Kb) de la SA para esta propuesta.

Valor por omisión: 50000

SA lifetime
La duración (en segundos) de la SA para esta propuesta.

Valor por omisión: 3600

ISAKMP-Action
Le solicita información acerca de la acción ISAKMP que se aplicará.

Name
El nombre de la acción ISAKMP.

Exchange mode
El tipo de modalidad de intercambio para las negociaciones de fase 1.

1 Principal

2 Agresivo

Valor por omisión: 1

Percentage of Minimum SA lifesize/lifetime
Duración mínima de la SA (como porcentaje) de la duración de la SA. No se aceptará una duración con un valor inferior a éste.

Valor por omisión: 75

ISAKMP connection lifesize
La duración (en Kb) de la conexión de fase 1. Cuando caduca la conexión de fase 1, la siguiente vez que se debe renovar la SA de la fase 2, la fase 1 vuelve a negociar completamente antes de que se inicie la fase 2.

Valor por omisión: 5000

ISAKMP connection lifetime
La duración (en segundos) de la conexión de fase 1. Cuando caduca la conexión de fase 1, la siguiente vez que se debe renovar la fase 2, la fase 1 se inicia completamente.

Valor por omisión: 5000

Negotiate SA automatically
Especifica si el SA se negocia automáticamente en la inicialización del sistema.

Yes o No

Valor por omisión: No

ISAKMP proposal
El nombre de la propuesta de ISAKMP (puede especificar hasta cinco propuestas) que se enviará o comprobará durante la modalidad rápida de fase 2. El orden en que se especifiquen determinará su prioridad: la primera será la superior.

ISAKMP-Proposal
Le solicita la información de propuesta de ISAKMP utilizada en las negociaciones de ISAKMP.

ISAKMP proposal name
El nombre de la propuesta de ISAKMP.

Authentication method
El tipo de autenticación que se utilizará durante las negociaciones de fase 1 de ISAKMP.

1 Clave precompartida

2 RSA SIG (modalidad certificada)

Valor por omisión: 1

Hash algorithm
El tipo de algoritmo hash que se utilizará durante las negociaciones de fase 1.

1 MD5

2 SHA

Valor por omisión: 1

Cipher algorithm
El tipo de algoritmo de cifras que se utilizará durante las negociaciones de fase 1.

1 DES

2 3DES

Valor por omisión: 1

Diffie Hellman Group ID
El tipo de grupo Diffie Hellman que se utilizará durante las negociaciones de fase 1.

1 Diffie Hellman Grupo 1

2 Diffie Hellman Grupo 2

Valor por omisión: 1

SA lifesize
La duración (en Kb) de la SA para esta propuesta.

Valor por omisión: 50000

SA lifetime
La duración (en segundos) de la SA para esta propuesta.

Valor por omisión: 5000

Policy
Le solicita información acerca de la configuración de la 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: Válido siempre

Name El nombre de configuración de la política

Priority
Prioridad relativa de esta política respecto a otras políticas (cuanto más alto es el número, más alta es la prioridad). Se utiliza para resolver conflictos si se aplican múltiples políticas a un paquete.

Valor por omisión: 5

Profile
El nombre de un perfil de tráfico de datos configurado anteriormente que se utilizará para esta política.

Validity period
El nombre de un período de validez configurado anteriormente que se utilizará para esta política.

IPSec action
Si esta política aplicará una acción IPSec, el nombre de una acción IPSec configurada anteriormente que se utilizará para esta política. Si especifica una acción IPSec segura, también debe especificar una acción ISAKMP.

ISAKMP action
El nombre de una acción ISAKMP configurada anteriormente que se utilizará para esta política. Si especifica una acción ISAKMP segura, también debe especificar una acción IPSec.

Diffserv action
Si desea correlacionar una acción DiffServ con esta política, el nombre de una acción DiffServ configurada anteriormente.

RSVP action
El nombre de una acción RSVP que aplicará esta política.

Profile

Le solicita información para definir un conjunto de selectores (condicionales) para un perfil de política en la que se llevarán a cabo acciones.

name

El nombre del perfil de política

ipv4-src-address-format

El formato de la dirección IPv4 de origen (rango, máscara de red, dirección única).

ipv4-src-address

La dirección IPv4 de origen (dirección baja si el formato de dirección es *rango*).

Valor por omisión: 0.0.0.0

ipv4-src-mask

La máscara IPv4 de origen (dirección alta si el formato de dirección es *rango*).

Valor por omisión: 255.0.0.0

ipv4-dest-address-format

El formato de la dirección IPv4 de destino (rango, máscara de red, dirección única).

ipv4-dest-address

La dirección IPv4 de destino (dirección baja si el formato de dirección es *rango*).

Valor por omisión: 0.0.0.0

ipv4-dest-mask

La máscara IPv4 de destino (dirección alta si el formato de dirección es *rango*).

Valor por omisión: 255.0.0.0

protocol-id

El id de protocolo en el que se realizará la filtración.

1 TCP

2 UDP

3 Todos los protocolos

4 Especificar rango

Valor por omisión: 3

src-port-start

El primer número de puerto del rango de números de puerto de origen.

Valor por omisión: 0

src-port-end

El último número de puerto del rango de números de puerto de origen.

Valor por omisión: 65535

dest-port-start

El primer número de puerto del rango de números de puerto de destino.

Valor por omisión: 0

dest-port-end
El último número de puerto del rango de números de puerto de destino.

Valor por omisión: 65535

src-id-type
El tipo de ID de origen, que se envía a la ubicación remota. Este valor se utiliza para determinar la política que contiene la información de ISAKMP necesaria durante las negociaciones de fase 1 de ISAKMP. Se compara con la información de la carga de útil de identificación del paquete ISAKMP. Esta información es necesaria si el igual remoto debe identificar el dispositivo con un valor distinto a la dirección IP.

1 Punto final de túnel local

2 Nombre de dominio completo del sistema principal

3 Nombre de dominio completo del usuario

4 ID de clave

any-user-access
Permite el acceso para cualquier usuario que se encuentre en la definición de perfil. Si ha especificado que No, se le solicitará el nombre del grupo de usuarios remotos de ese perfil. Este atributo sólo es necesario si quiere limitar el acceso de pares de acceso remoto a una política específica.

Yes o No

Valor por omisión: Yes

Received DS byte mask
La máscara de 8 bits que se aplicará al byte TOS de un paquete de entrada.

Valor por omisión: 0

Received DS byte match
El patrón de 8 bits para comparar el resultado de ANDing 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 interfaces específicas, es el nombre del grupo de pares de interfaces.

RSVP-Action
Le solicita información acerca de las acciones RSVP que se aplicarán.

Name
El nombre de la acción RSVP.

Permission
Especifica el nivel de permiso para las sesiones de RSVP que coinciden con esta acción.

1 Permitir

2 Denegar

Valor por omisión: 2

Max token rate
La cantidad máxima de ancho de banda (en Kbps) que RSVP asignará para un flujo individual.

Valor por omisión: 100

Max duration
La cantidad máxima de tiempo (en segundos) que puede durar un flujo (0 significa siempre).

Valor por omisión: 600

RSVP-to-DS
Especifica si se deben correlacionar los flujos de RSVP que coinciden con esta acción con una acción DiffServ configurada. RSVP utiliza la información de la acción DiffServ para marcar el byte TOS para el siguiente dispositivo de sentido inverso habilitado con DiffServ. Se utiliza en una red en la que los paquetes dejan una red habilitada con RSVP en una red habilitada con DiffServ.

Yes o No

Valor por omisión: No

VALIDITY-PERIOD
Le solicita información acerca del período de validez de la política y crea un perfil de política.

Name
El nombre del perfil de período de validez.

yyyymmddhhmmss:yyyymmddhhmmss
El período durante el cual son válidas las políticas que contiene este perfil de período de validez.

Ejemplo:

```
19980101000000:19981231000000
```

Months
Los meses durante los cuales son válidas las políticas que contienen este perfil de período de validez. Puede especificar cualquier secuencia de meses, utilizando las tres primeras letras de cada mes en inglés (por ejemplo jan o dec), con los meses separados por espacios o puede especificar `all` para indicar todos los meses del año.

Days
Las fechas en las que son válidas las políticas que contienen este perfil de período de validez. Puede especificar cualquier secuencia de días, utilizando las tres primeras letras de cada día en inglés (por ejemplo mon o fri), con los días separados por espacios o puede entrar `all` para especificar todos los días de la semana.

Starting time
La hora en que son válidas las políticas que contienen este perfil de período de validez. Especifique esta opción en el formato hh:mm:ss o * si quiere que la política sea válida todo el día.

Valor por omisión: *

Ending time
La hora en que caduca la validez de las políticas que contienen este perfil de período de validez. Especifique esta opción en el formato hh:mm:ss.

Valor por omisión: Ninguno

Change

Utilice el mandato **change** para cambiar la información en un objeto de política. Consulte la descripción del mandato **add** para los objetos disponibles.

Copy

Utilice el mandato **copy** para copiar información de un objeto de política a otro. Consulte la descripción del mandato **add** para los objetos disponibles. (El par de interfaces, el túnel manual y las opciones de usuario no se aplican al mandato copy.)

Delete

Utilice el mandato **delete** para suprimir información de un objeto de política. Consulte la descripción del mandato **add** para los objetos disponibles.

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 se inhabilitará.

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 se habilitará.

List

Utilice el mandato **list** para visualizar la información que desee de la configuración de política.

Sintaxis: list all
default-policy
ldap
refresh

All Muestra toda la información de la configuración de política.

Default-policy
Muestra el nombre de la política por omisión.

LDAP
Muestra los nombres de las configuraciones de LDAP definidas.

Refresh
Lista el estado de renovación de la política (habilitado o inhabilitado) y el tiempo del intervalo de renovación.

Mandatos de configuración del servidor de políticas de LDAP

Los mandatos de configuración del servidor de políticas de LDAP le permiten especificar las opciones del servidor LDAP para recuperar la información de política. La Tabla 39 resume los mandatos de configuración de LDAP y el resto de este apartado los describe detalladamente. Escríbalos en el indicador `Policy config>`. Puede entrar el mandato y las opciones en una línea o entrar sólo el mandato y responder a las indicaciones. Para ver una lista de opciones de mandato válidas, entre el mandato con un interrogante en vez de las opciones.

Tabla 39. Mandatos de configuración de LDAP

Mandato	Función
? (Ayuda)	Visualiza todos los mandatos disponibles para este nivel de mandato, o lista las opciones de mandatos específicos (si es que están disponibles). Consulte “Obtención de ayuda” en la página xxv.
Disable ldap	Inhabilita las opciones de configuración de LDAP.
Enable ldap	Habilita las opciones de configuración de LDAP.
Set ldap	Especifica las opciones de configuración de LDAP.
Exit	Hace volver al nivel de mandato anterior. Consulte “Salida de un entorno de nivel inferior” en la página xxv.

Disable LDAP

Utilice el mandato **disable ldap** para inhabilitar las funciones de búsqueda de políticas de LDAP del directorio.

Sintaxis: disable ldap
policy-search

policy-search
Inhabilita LDAP para el uso de funciones de búsqueda en el directorio.

Enable LDAP

Utilice el mandato **enable ldap** para habilitar las funciones de búsqueda de políticas de LDAP del directorio.

Sintaxis: enable ldap
policy-search

policy-search
Habilita LDAP para el uso de funciones de búsqueda en el directorio.

Set Default-Policy

Utilice el mandato **set default-policy** para especificar las opciones de política que se utilizarán mientras se renueva la base de datos de políticas. El mandato establece las opciones de manejo de errores y la seguridad por omisión necesaria para acceder al servidor de políticas de LDAP.

Sintaxis: set default-policy
default-error-handling
default-security

default-error-handling
Especifica las opciones de manejo de errores que se utilizarán mientras se renueva la base de datos de políticas.

Nota: El valor por omisión determina el comportamiento del dispositivo si se produce un error al reconstruir la base de datos de políticas. Si se produce un error, estas opciones determinarán el comportamiento del dispositivo. Son:

1. Restablecer la base de datos de políticas a la seguridad por omisión.
2. Desechar las normas leídas de LDAP, cargar las normas locales más la seguridad por omisión.

Estos valores sólo son válidos si se ha producido un error al crear la base de datos de políticas. Todas las opciones heredan la seguridad por omisión de desconexión o pase cuando se produce un error. Si selecciona la opción 2, todo el tráfico se desconecta o pasa a menos que coincida con una política definida localmente. Si la base de datos de políticas se crea satisfactoriamente, esta opción no se utiliza.

default-security
Especifica las opciones de seguridad que se utilizarán mientras se renueva la base de datos de políticas.

Nota: Una vez creada satisfactoriamente la base de datos de políticas, se define el comportamiento por omisión como en el pase. Esto significa que si el paquete no coincide con ninguna norma de política, se pasará libremente. Si quiere que los paquetes que no coincidan con una norma se desconecten globalmente o sólo para algunas interfaces, defina una política.

1 Aceptar y reenviar todo el tráfico de IP.

2 Permitir el tráfico de LDAP, rechazar el resto de tráfico de IP.

Si selecciona esta opción, se le solicitarán las direcciones IP locales del dispositivo en el que se enviará y recibirá el tráfico de LDAP.

3 Permitir y proteger el tráfico de LDAP, rechazar el resto de tráfico de 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 DH Grupo 1.

2 DH Grupo 2.

Phase1-Hash-Algorithm
El algoritmo hash que se utilizará durante las negociaciones de fase 1. El algoritmo hash proporciona la autenticación de los mensajes de la fase 1.

1 MD5.

2 SHA.

Phase1-Cipher-Algorithm
El algoritmo de cifras que se utilizará durante las negociaciones de fase 1. El algoritmo de cifras proporciona protección de cifrado para las negociaciones de fase 1.

1 DES

2 3DES

Phase1-Authentication-Method
El método de autenticación que se utilizará con el igual remoto. Especifica cómo ISAKMP determina si el igual remoto es actualmente el dispositivo correcto con el que negociar.

1 Clave precompartida

2 Certificado (RSA SIG)

Pre-Shared-Key-Value
Si ha especificado el método de autenticación de 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 IPSec permitido para la seguridad por omisión. Se le solicitará el algoritmo de autenticación que se utilizará durante las negociaciones de ISAKMP de fase 2.

0 Ninguno

1 HMAC-MD5

2 HMAC-SHA

Phase2-ESP-Cipher-Algorithm
ESP es el único protocolo IPSec permitido para la seguridad por omisión. Se le solicitará el algoritmo de cifrado que se utilizará durante las negociaciones de ISAKMP de fase 2.

1 ESP DES

2 ESP 3DES

3 ESP CDMF

4 ESP NULL

Primary-Tunnel-Start
La dirección IP del dispositivo que se utilizará para el tráfico de IKE e IPSec entre el dispositivo y la pasarela de seguridad que protege el servidor LDAP principal.

Primary-Tunnel-End
La dirección IP de la pasarela de seguridad remota que protege el servidor LDAP principal que se utilizará para el tráfico de IKE e IPSec.

Secondary-Tunnel-Start
La dirección IP del dispositivo que se utilizará para el tráfico de IKE e IPSec entre el dispositivo y la pasarela de seguridad que protege el servidor LDAP secundario.

Secondary-Tunnel-End
La dirección IP de la pasarela de seguridad remota que protege el servidor LDAP secundario que se utilizará para el tráfico de IKE e IPSec.

Set LDAP

Utilice el mandato **set ldap** para configurar los parámetros de funcionamiento de LDAP.

Sintaxis: set ldap anonymous-bind
yes
no
bind-name <*nombre*>
bind-pw <*contraseña*>

policy-base <*cadeana de caracteres*>
primary <*dirección ip*>
secondary <*dirección ip*>
version <*valor*>

anonymous-bind [Yes o No]
Especifica si se desea vincular con el directorio LDAP de forma anónima o con el nombre o contraseña de enlace que ha especificado.

Valor por omisión: Yes

bind-name <*nombre*>
Le solicita la información necesaria para vincularse al servidor LDAP antes de poder realizar una búsqueda en su directorio. El parámetro *nombre* especifica el nombre distintivo que utiliza el direccionador para identificarse. Si no entra este parámetro, se emite el mandato como una solicitud anónima.

bind-pw <*contraseña*>
Le solicita la información necesaria para vincularse al servidor LDAP antes de poder realizar una búsqueda en su directorio. El parámetro *contraseña* es la contraseña relacionada con el nombre distintivo. Si no entra este parámetro, se emite el mandato como una solicitud anónima.

policy-base <*cadena de caracteres*>
Le solicita que entre una serie de caracteres que se utilizará para definir el ámbito de la búsqueda para las políticas del servidor LDAP y SRAM del direccionador. Por ejemplo, puede utilizar esta opción para devolver políticas que sólo se aplican al direccionador A o para NHD o para IBM-US. La base de política es el nombre distintivo del objeto DeviceProfile en el servidor LDAP.

primary <*dirección ip*>
Le solicita la dirección IPv4 del servidor LDAP desde el cual se recuperan las políticas.

secondary <*dirección ip*>
Le solicita las direcciones IPv4 de un servidor LDAP de copia de seguridad que se utiliza si no se puede alcanzar el servidor por omisión.

version <*valor*>
Le solicita el número de versión de LDAP soportado por el servidor LDAP.

Valor por omisión: 2 (Los únicos valores aceptables son 2 o 3).

Set Refresh

Utilice el mandato **set refresh** para habilitar o inhabilitar la renovación automática de la base de datos de políticas una vez al día. Si se habilita, la base de datos de políticas se renueva una vez al día a la hora especificada. De esta forma se activan todos los direccionadores habilitados para políticas de la red para que incorporen automáticamente los cambios de política que se han producido en el directorio LDAP. Para restablecer este parámetro, utilice el mandato **reset refresh** de Talk 5 de la función de política.

Sintaxis: set refresh

enabled
yes
no
<*hora*>

enabled [yes o no]
Especifica si se realizará la renovación automática.

<hora>
Si ha habilitado el mandato, designa la hora del día (en formato de 24 horas) en la que se producirá la renovación.

Acceso al indicador de supervisión de la política

El fragmento de consola de la función de política le permite ver las políticas que se encuentran en la base de datos y 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 la política

Estos mandatos le permiten ver los perfiles definidos en la base de datos de políticas y habilitar o inhabilitar políticas individuales. La Tabla 40 resume los mandatos de supervisión de la política y el resto del apartado los describe. Escriba los mandatos en el indicador `Policy console>`. Puede entrar el mandato y las opciones en una línea o entrar sólo el mandato y responder a las indicaciones. Para ver una lista de opciones de mandato válidas, entre el mandato con un interrogante en vez de las opciones.

Tabla 40. Mandatos de supervisión de la política

Mandato	Función
? (Ayuda)	Visualiza todos los mandatos disponibles para este nivel de mandato, o lista las opciones de mandatos específicos (si es que están disponibles). Consulte “Obtención de ayuda” en la página xxv.
Disable	Inhabilita una política que está cargada en la base de datos de políticas.
Enable	Habilita una política que está cargada en la base de datos de políticas.
Reset	Renueva o restablece los criterios relacionados con la política.
Search	Comprueba o depura la actividad entre el servidor y el cliente LDAP.
Status	Muestra información acerca de la base de datos de políticas.
List	Muestra información acerca de la configuración de LDAP y las políticas definidas.
Test	Consulta el motor de políticas y recupera las normas que se han seleccionado
Exit	Hace volver al nivel de mandato anterior. Consulte “Salida de un entorno de nivel inferior” en la página xxv.

Disable

Utilice el mandato **disable** para inhabilitar una política que está cargada en la base de datos de políticas. Se aplicarán las decisiones predeterminadas a todos los paquetes de datos que inhabilite y que coincidan con los criterios de una política.

Sintaxis: disable *<nombre de política>*

Enable

Utilice el mandato **enable** para habilitar una política que está cargada en la base de datos de políticas. Se configurarán decisiones para las políticas aplicadas a todos los paquetes de datos que habilite y que coincidan con los criterios de una política.

Sintaxis: enable *<nombre de 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 la configuración de LDAP (tal como se especifica en el mandato **set ldap**) en la memoria. Los cambios serán activos para la siguiente operación de búsqueda. Este mandato también obliga a restablecer la base de datos de políticas e inactiva el tiempo de renovación de ésta.

policy-database
Renueva la base de datos de políticas. Detiene todos los túneles, SA de fase 1 y fase 2, restablece las estructuras de datos de RSVP y DiffServ y vacía la base de datos de políticas. Luego se cargan las políticas del servidor LDAP y se lleva a cabo un inicio automático. Mientras se reconstruye la base de datos, no se permitirá la entrada ni la salida de paquetes del direccionador a excepción de los paquetes que se dirijan o provengan del servidor LDAP.

refresh-time
Establecer la hora en que se renovará automáticamente cada día la base de datos de políticas. Si ha inhabilitado el tiempo de renovación, la base de datos no se renovará hasta que se rearranque o reinicie el direccionador.

Search

Utilice el mandato **search** para comprobar o depurar la actividad entre el servidor y el cliente LDAP. Puede realizar búsquedas en el directorio y que los resultados aparezcan 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 la información acerca de la base de datos de políticas.

Sintaxis: status

status
Muestra el resultado de la renovación más reciente de la base de datos de políticas, el tiempo que ha transcurrido desde la última renovación y la hora en que está programada la siguiente.

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 la información acerca de las políticas y configuraciones de LDAP.

Sintaxis: list default-policy
ldap
policy
refresh
rule
stats

default-policy
Lista la política por omisión utilizada durante las renovaciones de la base de datos de políticas.

ldap
Lista las configuraciones de LDAP en SRAM.

policy

basic Lista los componentes de la política por nombre de política lógica. Puede seleccionar una política o listarlas todas. El listado muestra los nombres de los componentes de políticas tal como se han entrado durante la configuración en Talk 6.

complete
Lleva a cabo la misma acción que list policy basic, sólo que el listado muestra la lista completa de todos los valores de parámetro de cada política lógica.

generated
Lleva a cabo la misma acción que list policy basic, sólo que el listado muestra los nombres de todas las normas generadas para cada política lógica.

refresh
Lista el estado de renovación de la política (habilitado o inhabilitado) y el tiempo del intervalo de renovación.

rule
Lista la información acerca de las normas generadas según las siguientes opciones:

basic Lista todas las normas generadas. Puede seleccionar una norma de la lista o listarlas todas. El listado muestra los nombres de los componentes de las normas. Los componentes son:
policy name

loaded from (LDAP or local)

state
priority

number of hits

profile

validity (seguido de una lista de acciones que consta de las siguientes)
IPSec (and, or)
ISAKMP (and, or)
DiffServ (and, or)
RSVP

complete
Lleva a cabo la misma acción que rule basic, sólo que el listado muestra los nombres de todos los parámetros para cada componente.

stats
Lista las normas que se han cumplido y el número de veces. Una norma puede tener diversas acciones y es posible que no se hayan cumplido todas las acciones, por lo que esta opción indica también la acción de la norma que se ha cumplido y el número de veces.

Test

Utilice el mandato **test** para verificar el comportamiento de la base de datos de políticas. Le permite entrar un conjunto de selectores que consulta el motor de políticas y recupera las normas que deben coincidir. Se le solicitan las direcciones de origen y destino, los puertos de origen y destino, el ID de protocolo y el valor de TOS. Si coincide una norma, el mandato devuelve el nombre de la norma. Si no, indica *No match found.*

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 política que produciría esta consulta. El tipo de política devuelta podría incluir la información de DiffServ, información de fase 1 y 2 de IKE y los ID de túnel manual de IPSec.

ISAKMP
Simula una consulta de base de datos de IKE para la información de política de fase 1 y devuelve las decisiones de política que produciría esta consulta. Si utiliza esta opción, deberá establecer las direcciones de origen y destino en las direcciones IP de punto final del túnel, el protocolo en 17 y los puertos de origen y destino en 500.

IPSec
Simula una consulta de base de datos de IKE para la información de política de fase 2 y devuelve las decisiones de política que produciría esta consulta. Si utiliza esta opción, deberá establecer las direcciones de origen y destino en las direcciones IP de punto final del túnel, el protocolo en 17 y los puertos de origen y destino en 500.

RSVP

Simula una consulta de base de datos de RSVP y devuelve las decisiones de política de RSVP que produciría esta consulta.

Mandatos de supervisión de la política (talk 5)

Capítulo 20. Utilización de la seguridad IP

Este capítulo explica cómo utilizar la función de Seguridad IP e incluye los siguientes apartados:

- "Visión general de la seguridad IP"
- "Conceptos de seguridad IP" en la página 336
- "Utilización del Intercambio de claves de Internet" en la página 345
- "Utilización de la Infraestructura de claves públicas" en la página 347
- "Utilización de la seguridad IP manual (IPv4)" en la página 352
- "Utilización de la seguridad de IP manual (IPv6)" en la página 352

Visión general de la seguridad IP

Este apartado proporciona una visión general de las posibilidades de seguridad IP tanto para IPv4 como para IPv6.

Utilización de los túneles protegidos

Para proteger los paquetes IP enviados a otro sistema principal, direccionador o cortafuegos, puede configurar un túnel protegido para cada ruta IP que deba estar protegida. Un túnel IPSec es una conexión lógica de dos vías hacia el sistema principal remoto, direccionador o cortafuegos a través del cual el direccionador envía paquetes IP protegidos. Los túneles protegidos se identifican por parámetros como las direcciones del sistema principal de origen y destino, números de puerto e ID de túnel.

Con IPv4 puede definir un túnel negociado configurando una política de túnel en la base de datos de políticas o crear un túnel manual mediante el mandato **add tunnel** de Talk 6 como se muestra en el apartado "Configuración del túnel para el direccionador A" en la página 368. Con IPv6, utilice el mandato **add tunnel** de Talk 6.

Para establecer un túnel IPSec protegido, una política puede especificar la función AH (Authentication Header) de IP (consulte el apartado "Cabecera de autenticación de IP" en la página 338), que conecta las cabeceras de autenticación especiales, y la función ESP (Encapsulation Security Payload) (consulte el apartado "Carga útil de seguridad de encapsulación de IP" en la página 339), que cifra los datos. La política establece que se implementen las siguientes medidas de seguridad para los paquetes:

- Claves de autenticación de AH y algoritmo AH (consulte el apartado "Configuración de los algoritmos" en la página 358 o el "Configuración de los algoritmos" en la página 370 según sea apropiado).
- Claves de cifrado y descifrado de ESP y algoritmo de cifrado de ESP (consulte el apartado "Configuración de los algoritmos" en la página 358 o el "Configuración de los algoritmos" en la página 370 según sea apropiado).
- Índices de parámetros de seguridad (SPI) (consulte el apartado "Asociaciones de seguridad" en la página 340).

Nota: Para cada túnel de seguridad, el remitente y el destinatario deben seleccionar opciones idénticas.

Conceptos de seguridad IP

Los paquetes enviados mediante el Protocolo Internet (IP) pueden protegerse mediante la función Seguridad IP del 2212.

La seguridad, tal como se define en RFC 2401 - Arquitectura de la seguridad para el Protocolo Internet, consta de las siguientes funciones:

Autenticación
Confirmación de que los datos recibidos son los mismos que los datos enviados y que el remitente especificado es realmente el remitente.

Integridad
Confirmación de que los datos se han transmitido del origen al destino sin alteración no detectada.

Confidencialidad
Comunicación en la que los destinatarios reales saben lo que se ha enviado, pero que no permite a terceros determinarlo.

No rechazamiento
Comunicación en la que el destinatario puede verificar que el remitente ha enviado ciertos datos aunque el remitente niegue más tarde haberlos enviado.

Nota: En algunos países, no se proporciona el soporte de cifrado debido a las regulaciones de exportación de EE.UU. y no se visualizan los parámetros de cifrado. Sin embargo, el algoritmo ESP-NULL siempre está disponible. Para ver la definición del algoritmo ESP-NULL, consulte el apartado “Algoritmos de cifrado de ESP” en la página 339.

Terminología de seguridad IP

Se utilizan los siguientes pasos al describir los temas de IPSec relacionados con IPv4:

AH (Authentication Header)
Área de datos que contiene información de cabecera del paquete y que proporciona la autenticación de origen de datos, integridad de los datos y protección de repetición.

Certificado
Elemento de datos de codificación ASN.1 (según los estándares ITU X.509) que enlaza el ID de una entidad final con su clave pública. (En este caso, la entidad final es la entidad de negociación de ISAKMP.) La entidad final debe registrar el ID y clave pública con una autoridad de certificados (CA) sometiendo una solicitud de certificado. La CA verifica la solicitud, la firma y la emite a la entidad. ISAKMP utiliza el certificado de clave pública durante el procesamiento de fase 1 para autenticar los intercambios de mensajes iniciales que configuran la clave secreta original (clave criptográfica) entre direccionadores.

Autoridad de certificados (CA)
Una autoridad fiable que emite certificados digitales X.509 “firmados” que deben utilizar los usuarios para intercambiar datos de usuario seguros mediante ISAKMP. Para participar en intercambios de datos seguros con otras partes habilitadas para ISAKMP, el direccionador se debe registrar en una CA y obtener un certificado digital X.509 para utilizarlo en la autenticación.

Firma digital
Elemento de datos que contiene un ID codificado de usuario que forma parte de un certificado digital X.509. Los usuarios intercambian certificados durante las negociaciones de fase 1 para autenticarse mutuamente. La firma se genera mediante una operación de claves públicas en un área de datos de entrada que se firmará.

ESP (Encapsulating Security Payload)
Función de IPSec que puede encapsular y cifrar un datagrama de forma que sólo el destinatario y nadie más puede determinar el contenido. Comprende la integridad de los datos y la protección de repetición. La ESP también proporciona autenticación de origen de los datos. Funciona en las siguientes modalidades: modalidad de transporte, que cifra sólo la carga útil del datagrama original y deja la información de dirección visible a las partes no autorizadas y la modalidad de túnel, en la que se cifra todo el datagrama original, incluida la cabecera. Oculta la información de dirección sensible.

IKE (Internet Key Exchange)
Protocolo derivado de los protocolos ISAKMP y Oakley, que utiliza la comunidad Internet para intercambiar claves criptográficas y autenticar las partes de una comunicación.

ISAKMP
Internet Security Association and Key Management Protocol. Esta función configura automáticamente las asociaciones de seguridad y gestiona claves criptográficas de paquetes durante un intercambio de datos.

MIB (Management Information Base)
Bloque de datos enviados por un direccionador como respuesta a una consulta de una autoridad fiable central que ha solicitado información estadística acerca de las operaciones del direccionador. La autoridad puede detectar problemas en la red y ponerse en contacto con una parte responsable para corregir la acción.

Oakley
Protocolo de gestión de claves criptográficas utilizado por ISAKMP.

PFS (Perfect Forward Secrecy)
Nivel de seguridad de datos obtenido si las negociaciones de fase 2 proporcionan información de claves criptográficas nueva para cada negociación. ISAKMP lo consigue habilitando el intercambio de valores de Diffie Hellman públicos entre las partes. Esta función de seguridad evita que cualquiera determine una clave criptográfica actual de una clave concedida anteriormente.

Negociaciones de fase 1
Comunicación entre un remitente y un destinatario que establece una asociación de seguridad y claves criptográficas de ISAKMP que protegen los mensajes ISAKMP que se intercambiarán durante las negociaciones de fase 2. La fase 1 es intensiva para el procesador y no se suele realizar con frecuencia, tal vez sólo diaria o semanalmente.

Negociaciones de 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 del usuario. Estas negociaciones se suelen producir frecuentemente, cada dos o tres minutos, y se utilizan para renovar las claves criptográficas regularmente sin la intervención del usuario.

Proxy
Direccionador que se asigna para funcionar en nombre de otro dispositivo de la red.

Infraestructura de claves públicas (PKI)
Marco que utiliza una CA para enlazar los ID de usuario con su clave pública y distribuye la clave pública del enlace de forma que asegure su protección.

Modalidad rápida
Término utilizado para describir las negociaciones de fase 2 para asociaciones de seguridad que no son de ISAKMP.

Repetición
Acto de captura de un datagrama y el intento de determinar su contenido o montar un ataque de negación de servicio reenviándolo repetidamente.

Asociación de seguridad (SA)
Área de datos que reúne información acerca de un paquete de datos, por ejemplo su algoritmo criptográfico e información de claves, las identidades de las partes participantes, etc.

Transformación
Colección nombrada de información acerca de una configuración de selecciones de autenticación y cifrado.

Cabecera de autenticación de IP

La Cabecera de autenticación (AH) se describe en la Cabecera de autenticación de IP RFC 2402. Esta cabecera contiene datos de autenticación para el datagrama de IP.

Para IPv4 con IPSec negociado, la política asignada a un datagrama implementa una función de autenticación criptográfica que confía en el protocolo IKE (Internet Key Exchange) y del par de claves pública/privada. Para los túneles manuales IPv4 y para IPv6, el remitente utiliza una función criptográfica que confía en una clave de autenticación secreta. En cualquier caso, la función de autenticación criptográfica se aplica al contenido del datagrama. Puede especificar AH solo o con ESP. Consulte el apartado “Utilización de AH y ESP” en la página 339 para obtener detalles.

Algoritmos de autenticación de AH

Los túneles protegidos que utilizan la política de túnel de AH deben utilizar uno de los siguientes algoritmos de autenticación:

- Autenticación de IP HMAC-MD5 con prevención de repetición
- Autenticación de IP HMAC-SHA-1 con prevención de repetición

Estos algoritmos AH combinan una función de autenticación de mensajes con clave utilizando el código hash criptográfico (hashed message authentication code, abreviado como HMAC) con una función de prevención de repetición opcional. La prevención de repetición utiliza un número de secuencia incluido en la AH para verificar que no se ha recibido anteriormente un paquete. La prevención de repetición protege al destinatario de los ataques de negación de servicio, en los que se envía repetidamente el mismo paquete y el direccionador está tan ocupado procesando paquetes duplicados que no puede procesar el tráfico legítimo. Se aplica un código de autenticación a una clave criptográfica secreta y los datos, luego a la salida de la clave secreta y la salida de la primera operación. Consulte la Figura 32 en la página 339 para ver una muestra de cómo se realiza para HMAC-MD5.

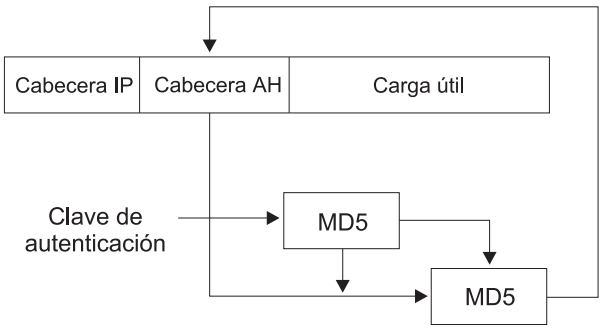


Figura 32. Creación de un mensaje autenticado por MD5 de HMAC

Carga útil de seguridad de encapsulación de IP

La ESP (Encapsulating Security Payload) de IP se describe en Carga útil de seguridad de encapsulación de IP RFC 2406. ESP cifra una parte o todo el paquete IP para proporcionar confidencialidad además de autenticación (opcional) e integridad. Sin embargo, si selecciona el algoritmo ESP-NULL, ESP realiza sólo la autenticación y comprobación de la integridad. Puede especificar ESP solo o con AH. Consulte el apartado "Utilización de AH y ESP" para obtener detalles.

Algoritmos de autenticación de ESP

Los algoritmos disponibles para la autenticación de ESP son los mismos que los de AH, mostrados anteriormente en el apartado "Algoritmos de autenticación de AH" en la página 338.

Algoritmos de cifrado de ESP

Los túneles protegidos que utilizan la política de cifrado de ESP deben utilizar uno de los siguientes algoritmos de autenticación o el algoritmo ESP_NULL:

- DES-CBC (Data Encryption Standard in Cipher Block Chaining Mode)
- CDMF (Commercial Data Masking Facility)
- 3DES (Triple DES)

Nota: A excepción de ESP-NULL, los algoritmos de cifrado de ESP están sujetos a las leyes de exportación de EE.UU. Si el 2212 no le permite utilizar algunos de estos algoritmos, es posible que la venta de éstos esté prohibida en su país. Consúltelo con el representante de IBM para obtener más información.

El algoritmo ESP-NULL no cifra los datos de texto plano y está disponible en todos los países. Habilita sólo la autenticación de ESP y la comprobación de la integridad, no el cifrado. Si utiliza ESP-NULL, ***debe*** utilizar uno de los algoritmos de autenticación de ESP.

Utilización de AH y ESP

Un túnel protegido 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, las siguientes sentencias son aplicables:

- La política AH-ESP especifica que para los paquetes de salida, el cifrado se ejecuta antes de la autenticación. En este caso, en el direccionador de destino

se ejecuta primero la función de autenticación de AH, comprobación de paquetes de entrada y sólo los paquetes que pasan la autenticación se reenvían al ESP para la descifrado.

- La política ESP-AH especifica que para los paquetes de salida, la autenticación se ejecuta antes del cifrado. En este caso, en el direccionador de destino la función ESP descifra primero los paquetes de entrada y sólo los paquetes que se descifran satisfactoriamente se reenvían para la autenticación de AH.

Asociaciones de seguridad

Una Asociación de seguridad (SA) es una "conexión" simple que proporciona servicios de seguridad al tráfico que gestiona. Los servicios de seguridad se proporcionan a una SA mediante el uso de AH o ESP, pero no ambos. Si se aplica tanto la protección de AH como de ESP a una corriente de tráfico, se crean dos (o más) SA para proporcionar protección a la corriente. Para proteger la comunicación bidireccional típica entre dos sistemas principales o dos pasarelas de seguridad, son necesarias dos SA (una en cada dirección).

Modalidad de túnel y modalidad de transporte

La modalidad operacional (túnel o transporte) determina la manera como IPSec maneja los paquetes de IP. La modalidad de túnel es el valor por omisión y es obligatorio si el direccionador actúa como pasarela de seguridad. Protege los datos en un solo segmento de una vía de acceso a través de una red. La modalidad de transporte está permitida sólo cuando el direccionador actúa como sistema principal y protege los datos de extremo a extremo, a lo largo de una vía de acceso completa.

Modalidades AH y operacional

En la modalidad de túnel, la AH se coloca en la parte frontal del paquete de IP y se crea una cabecera de IP nueva que se coloca frente a la AH. La cabecera de IP del paquete que se coloca en el túnel (cabecera interior) incluye las direcciones definitivas de origen y destino del paquete. La cabecera de IP nueva (cabecera exterior) pude contener las direcciones de las pasarelas de seguridad, que son puntos finales del túnel. La AH protege todo el paquete nuevo, tanto la cabecera de IP nueva como el paquete de IP que se coloca en el túnel, excepto los cambios mudables de la cabecera de IP nueva.

En la modalidad de transporte, la AH se inserta después de la cabecera de IP y antes de la cabecera de un protocolo de la capa superior, por ejemplo TCP o UDP. En esta modalidad, la AH autentica la cabecera de protocolo de la capa superior y el contenido del paquete de IP, excepto los campos mudables de la cabecera de IP (como el tiempo de vida [TTL], suma de comprobación, distintivo de fragmentos, desplazamiento de fragmentos y tipo de servicio [TOS]).

La Figura 33 en la página 341 muestra el formato de los datagramas de AH protegida.

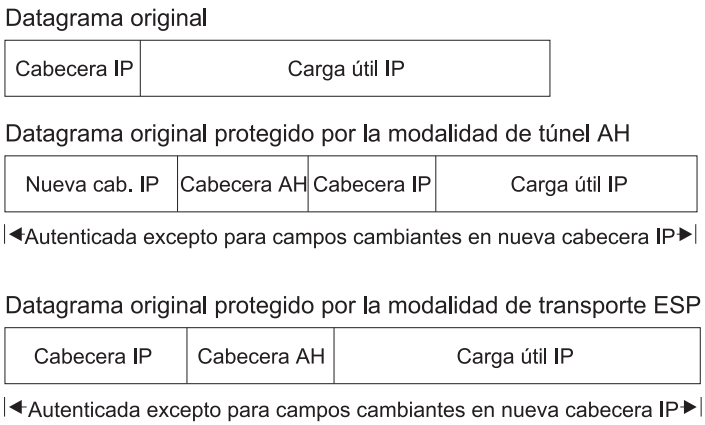


Figura 33. Formato de datagramas de AH protegida

Modalidades ESP y operacional

En la modalidad de túnel, los datos de carga útil contienen todo el paquete de IP y se crea una cabecera de IP nueva que se coloca frente a la cabecera de ESP. La cabecera de IP del paquete que se coloca en el túnel (cabecera interior) contiene las direcciones definitivas de origen y destino del paquete, mientras que la cabecera de IP nueva (cabecera exterior) contiene las direcciones de las pasarelas de seguridad. ESP cifra el paquete de IP que se coloca en el túnel. Si utiliza la autenticación de ESP, se autentican la cabecera de ESP, el paquete de IP que se coloca en el túnel y la cola de ESP.

En la modalidad de transporte, los datos de carga útil contienen los datos de protocolo de la capa superior cifrados, por ejemplo los datos de TCP o UDP. Si utiliza la autenticación, se autentican la cabecera de ESP, los datos de protocolo de la capa superior y la cola de ESP.

La Figura 34 muestra el formato de los datagramas de ESP protegido.

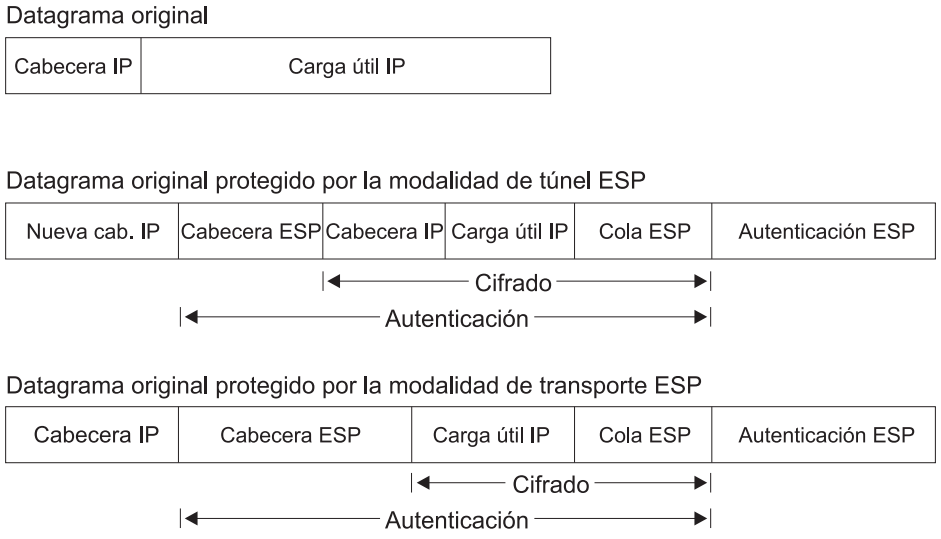


Figura 34. Formato de datagramas de ESP protegido

Jerarquización de AH y ESP

Puede anidar un protocolo dentro de otra instancia de sí mismo o de otro protocolo. La Figura 35 en la página 342 muestra los efectos de la anidación de un datagrama de ESP protegido dentro de un túnel de AH.

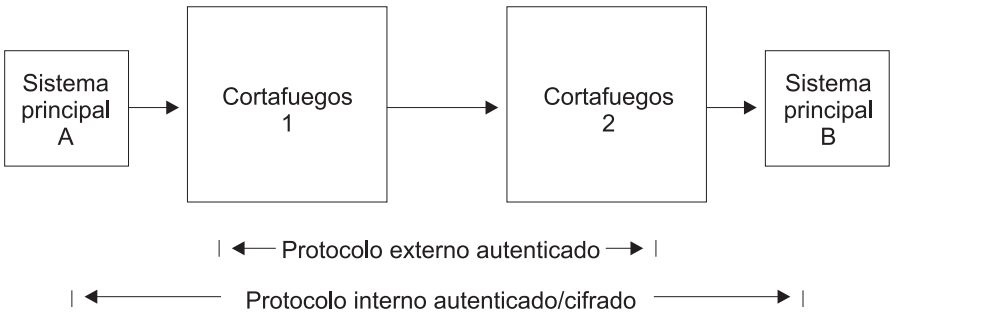


Figura 35. Anidación de ESP dentro de un túnel de AH

Utilización de la seguridad IP con paquetes L2TP

Con IPv4, también puede utilizar IPSec para proteger paquetes L2TP. Después de crear un túnel L2TP encapsulando un marco L2TP dentro de un paquete UDP, puede encapsular el paquete UDP dentro de un paquete de IP cuyas direcciones de origen y destino definan los puntos finales del túnel. Luego puede aplicar los protocolos AH, ESP y ISAKMP al paquete de IP. La Figura 36 muestra un paquete L2TP de IP encapsulado que incluye PPP y su protocolo de carga útil para la transmisión a través de Internet.

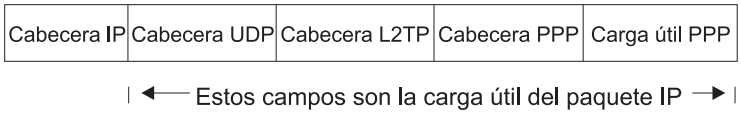


Figura 36. Paquete de L2TP de IPSec protegido

Modalidad de túnel en túnel

Para una mayor seguridad, además de las funciones de seguridad tratadas anteriormente, puede encapsular los paquetes de una corriente de tráfico dos veces y transmitirlos primero a través de un túnel IPSec y luego a través de otro (túnel en túnel).

Nota: El uso del cifrado múltiple (utilizando la modalidad de túnel en túnel cuando se realiza el cifrado para ambos túneles) dentro del direccionador está restringido por las regulaciones de exportación del gobierno de EE.UU.Sólo se da soporte a esta opción en las cargas de software que se encuentran bajo un control estricto de exportación (cargas de software que dan soporte a RC4 con claves de 128 bits y Triple DES).

Con IPv4, una norma de la base de datos de políticas designa un paquete para la encapsulación (interior) para el primer túnel, y antes de que se envíe el paquete, la norma hace que se envíe el paquete a un segundo túnel para una segunda encapsulación (exterior). Con IPv6, una norma de control de acceso de filtro de paquetes identifica un paquete para la encapsulación (interior) para el primer túnel, y antes de que se envíe el paquete, una segunda norma hace que se envíe el paquete a un segundo túnel para una segunda encapsulación (exterior).

Los dos túneles IPSec se originan en el mismo direccionador y los extremos remotos de los túneles se encuentran en la misma ubicación física, pero en distintas máquinas. El extremo remoto del primer túnel puede ser una pasarela o un sistema principal protegidos; el extremo remoto del segundo túnel *debe* ser un direccionador de pasarela protegido. Puesto que los túneles tienen diferentes destinos, deben tener direcciones IP remotas distintas. Los dos túneles utilizados para el túnel en túnel deben estar configurados para la modalidad de túnel y no se permite el relleno adicional en el segundo túnel.

Cuando se ha encapsulado dos veces, el paquete se transmite a través del segundo túnel (exterior). Al final de ese túnel, se elimina la encapsulación externa y el paquete se reenvía al primer túnel (interno), según la información de la cabecera creada por la encapsulación del primer túnel. Al final de este túnel, se elimina la encapsulación interna y el paquete se reenvía al destino final.

Descubrimiento de la unidad de transmisión máxima de la vía de acceso

Para IPv4 y IPv6, IPSec da soporte al Descubrimiento de PMTU (Unidad de transmisión máxima de la vía de acceso) si el 2212 actúa como pasarela de seguridad. El soporte del Descubrimiento de PMTU es interesante si no se puede fragmentar un paquete. Con IPv4, los paquetes no se pueden fragmentar si tienen establecido el bit de no fragmentación (DF). Con IPv6, los direccionadores intermedios no pueden fragmentar los paquetes. En estas situaciones, si el paquete no cabe en un enlace de la vía de acceso de un extremo del túnel protegido al otro, se envía un mensaje de error de ICMP de “paquete demasiado grande” al autor del paquete.

Puesto que el direccionador actúa como una pasarela de seguridad, el paquete con el error se devuelve al direccionador de origen en vez de al autor verdadero del paquete. El direccionador de recepción debe pasar la MTU al autor verdadero, quien reducirá el tamaño del paquete para que pueda llegar al destino final. El soporte para el descubrimiento de PMTU se trata en RFC 2401 - Arquitectura de seguridad para el Protocolo Internet.

IPv4 proporciona las siguientes opciones para el valor de bit DF en la cabecera exterior del paquete que se ha colocado en el túnel:

1. Copiar de la cabecera interior
2. Siempre establecido
3. Siempre libre

Estas opciones están disponibles al configurar la modalidad de túnel en túnel, por ejemplo utilizando la función de política **add ipsec-manual-tunn** (IPv4) o el mandato **add tunnel** (IPv6) de Talk 6. El bit DF se maneja según la opción seleccionada excepto bajo estas condiciones:

- 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 del paquete encapsulado es mayor que la MTU mínima.

En estas circunstancias, para IPv4, el bit DF no está establecido, independientemente de la configuración, y el paquete protegido se puede fragmentar según sea necesario en la vía de acceso al receptor. Para IPv6, el paquete se fragmenta según sea necesario cuando sale de la pasarela de seguridad para que quepa en la PMTU del túnel. Esta acción especial es necesaria porque el paquete de entrada ya es menor o igual que la MTU mínima, por lo que el sistema principal de origen no disminuirá el tamaño. Si la fragmentación no estuviera permitida, esta paquete no llegaría nunca a su destino final

Puesto que los cambios en la configuración o la topología de la red pueden cambiar la PMTU, el valor de PMTU debe caducar periódicamente y restablecerse al máximo. El valor por omisión de temporizador de caducidad es de 10 minutos y se puede configurar con el mandato **set path** de Talk 6. Si se establece el parámetro de caducidad en 0 se inhabilita la caducidad de la PMTU.

Diagrama de una red con un túnel de seguridad IP

La Figura 37 muestra un ejemplo de una red con dos túneles IPSec que conectan el direccionador A (con IPSec) al direccionador B (con IPSec y Conversión de direcciones de red para IPv4).

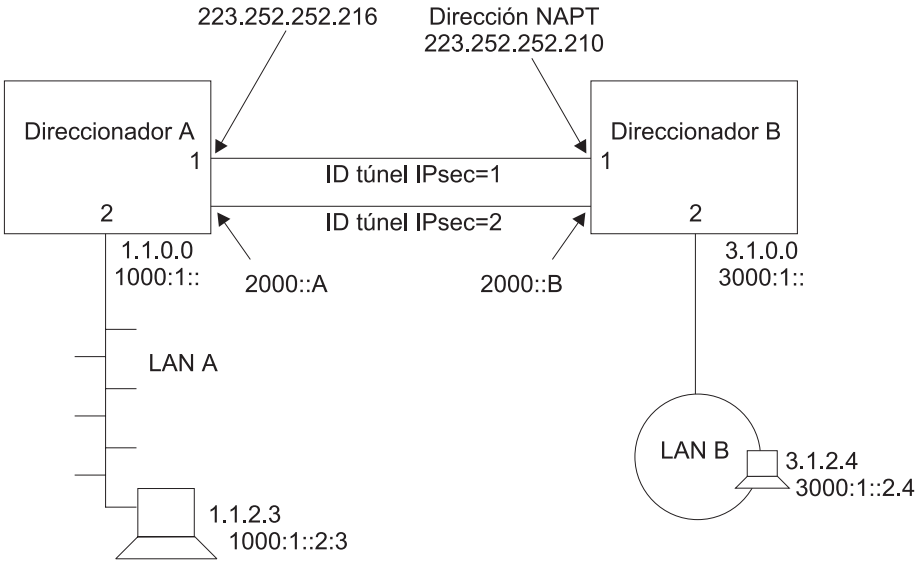


Figura 37. Red con IPSec y NAT

En esta red, se ha configurado un túnel IPSec con ID de túnel IPSec 1 de la dirección IPv4 223.252.252.216 del direccionador A a la dirección IPv4 223.252.252.210 del direccionador B. Se ha configurado el direccionador A para IPSec. Se ha configurado el direccionador B para IPSec y NAT.

También en esta red, se ha configurado un túnel IPSec con ID de túnel IPSec 2 de la dirección de IPv6 2000::A del direccionador A a la dirección de IPv6 2000::B del direccionador B.

Con IPv4, si desea configurar esta red para IKE, siga los pasos que empiezan en el apartado "Configuración del intercambio de claves en Internet (IPv4)" en la página 353. Para IPv4 con IPSec manual, siga los pasos que empiezan en el apartado "Configuración de un túnel manual (IPv4)" en la página 368. Para IPv6, siga los pasos que empiezan en el apartado "Configuración de un túnel manual (IPv6)" en la página 371.

Nota: Aunque no tenga previsto utilizar NAT en la red, la descripción de configuración del direccionador B puede ayudarle a comprender mejor la relación entre los parámetros de cada extremo del túnel IPSec.

Utilización del Intercambio de claves de Internet

Este apartado explica la manera de utilizar el Intercambio de claves de Internet (IKE) para automatizar la definición y creación de asociaciones de seguridad de IPSec (SA). IKE es un estándar soportado por el IETF (RFC 2409) que proporciona a los productos habilitados para IPSec del mismo proveedor o de proveedores distintos una forma estándar para comunicarse acerca de los requisitos de seguridad.

IKE proporciona un marco en el cual se cumplen los siguientes requisitos de seguridad:

Autenticación de la entidad de negociación remota (igual de IKE)
A través del uso de una clave precompartida o un certificado digital, IKE autentica la identidad de la entidad con la que se está comunicando al hacer que la entidad demuestre que es quien dice ser.

Creación de material de claves idéntico en ambos iguales
Si se utiliza el mecanismo de claves públicas y privadas de Diffie-Hellman, IKE proporciona el intercambio del componente de claves públicas y la generación independiente de claves idénticas para cada igual.

Proporciona protección para la negociación de asociaciones de seguridad de IPSec
A través de un proceso de dos fases, descrito en el siguiente tema, IKE proporciona la creación de asociaciones de seguridad que se utilizan sólo para proteger la negociación de los *túneles* de IPSec, y la negociación y creación de *asociaciones de seguridad* que IPSec utiliza para proteger los datos del usuario.

Fases del Intercambio de claves de Internet

IKE define dos intercambios de negociación distintos: la fase 1 y la fase 2. La fase 1 configura un túnel seguro entre los dos iguales de IKE, que proporcionará protección para las negociaciones de túnel IPSec siguientes. Las siguientes acciones se producen durante la fase 1 en el orden que se muestra:

1. Los iguales de 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 de IKE*, al algoritmo hash que se utilizará, el método de autenticación y el grupo Diffie-Hellman que se utilizará al generar claves.

2. Las claves Diffie-Hellman se generan y las partes públicas se intercambian con el igual de IKE. Estas claves se utilizan para generar claves de cifrado que cifrarán las negociaciones de fase 1 y permitirán también la generación de claves que utilizarán los túneles IPSec.
3. El igual IKE se autentica utilizando uno de estos dos métodos soportados—modalidad de clave precompartida y modalidad de firma.

   En la modalidad de clave precompartida, los dos iguales de IKE, mediante un proceso de fuera de línea previo, han intercambiado una clave y ésta se utiliza durante la fase 1 para autenticar el igual. La clave precompartida se configura mediante el mandato **add user** de la función de política.

   En la modalidad de firma, se utiliza un certificado digital X.509 para proporcionar las claves que se utilizan para cifrar y descifrar las cargas útiles de los mensajes de fase 1. La firma y verificación satisfactoria comprende la autenticación del igual. Para ver una descripción detallada de la modalidad de firma y el uso de certificados digitales X.509, consulte el apartado. “Utilización de la Infraestructura de claves públicas” en la página 347.

Las negociaciones de fase 1 pueden producirse a través de una de estas dos modalidades de intercambio:

- La modalidad principal utiliza seis mensajes para llevar a cabo las negociaciones de fase 1 y cifra las identidades de los iguales de la negociación.
- La modalidad agresiva utiliza tres mensajes para llevar a cabo las negociaciones de la fase 1. Los iguales intercambian las identidades no protegidas en los dos primeros mensajes.

Negociación de un túnel de seguridad IP

El proceso descrito en este tema se produce cuando un direccionador se prepara para enviar un paquete cuyos atributos coinciden con los definidos en una norma de una base de datos de políticas. La negociación de un túnel se produce en dos fases. Durante la fase 1, el direccionador de envío inicia la comunicación transmitiendo el primer mensaje de un intercambio de seis mensajes, lo que establece las opciones de seguridad que se utilizarán durante la fase 2. El receptor responde y las dos partes negocian las características de la asociación de seguridad (SA) de ISAKMP y los algoritmos de autenticación y cifrado que se utilizarán, y autentican mutuamente su identidad. Durante la fase 2, las partes intercambian un total de tres mensajes para negociar las SA y las claves que se utilizarán para proteger los datagramas de IP que se envían entre sí. La fase 1 sigue de esta manera:

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 qué opciones de seguridad da soporte.
3. Mensaje 3: El remitente transmite el valor público de Diffie Hellman y un valor aleatorio desde el que se crearán las claves de cifrado.
4. Mensaje 4: El receptor transmite su propio valor público de Diffie Hellman y un valor aleatorio desde el que se crean las claves de cifrado. En este momento, las dos partes crean claves públicas y privadas e información relacionada con las claves que se utilizará en los intercambios de mensajes de ISAKMP.

5. Mensaje 5: El remitente transmite una autorización digital y puede incluir un certificado digital X.509 firmado por una autoridad de certificados fiable (CA). Si el remitente no incluye un certificado válido, el receptor debe utilizar el protocolo LDAP para obtener un certificado de un CA fiable, un servidor de DNS seguro, una antememoria local que correlaciona los certificados utilizados anteriormente con sus valores de ID respectivos o puede solicitar un certificado de un remitente, quien debe enviarlo inmediatamente.
6. Mensaje 6: Después de verificar la firma digital del remitente, el receptor transmite el mismo tipo de información de identificación sobre sí mismo al remitente.

En este momento, las dos partes se han autenticado mutuamente, han acordado las características de la SA y han producido claves e información relacionada con las claves para manejar SA de ISAKMP. Ahora las partes entran en la fase 2 para negociar las claves y SA que no son de ISAKMP, que se utilizarán para proteger los datagramas de IP intercambiados. La fase 2 sigue de esta manera:

1. Mensaje 1: El remitente propone una SA que no es de ISAKMP transmitiendo una selección de algoritmos ESP o AH e incluye también otra información relacionada con la seguridad.
2. Mensaje 2: El receptor indica al remitente la propuesta que ha seleccionado e incluye información relacionada con 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 claves públicas

Este apartado explica cómo utilizar la infraestructura de claves públicas (PKI). A través de PKI, IKE soporta la modalidad de claves públicas para la autenticación de entidades de IKE. Aunque esta versión da soporte a la modalidad de clave precompartida, que no requiere el soporte a PKI, esta modalidad contiene una desventaja inherente. Para la autenticación, requiere la configuración de cada una de las entidades de IKE con la clave precompartida de cada uno de los iguales. Esto limita enormemente la escalabilidad de las operaciones de IKE. La firma basada en claves públicas o la modalidad de cifrado proporcionan una escalabilidad mucho mejor. En esta versión, el certificado digital X.509 se utiliza en las negociaciones de fase 1 de IKE de la modalidad de firma para autenticar las entidades de IKE.

Asigne una identidad a cada entidad IKE que quiera que participe en las negociaciones de IKE especificando un valor exclusivo en el campo de ID de ISAKMP cuando configure el perfil de políticas del usuario. Cada entidad de IKE autentica su identidad con sus iguales.

PKI se está definiendo y desarrollando para dar soporte a la operación de claves públicas. En PKI, un certificado digital X.509 enlaza la clave pública de una entidad con su identidad establecida. Una entidad de IKE puede extraer la clave pública incluida en un certificado. Puede llevar a cabo una operación de claves públicas para autenticar la identidad de un igual que participa en una negociación de IKE. Se utiliza una clave pública para la modalidad de firma de IKE. En esta modalidad, el firmante utiliza su clave privada para firmar la firma digital. El receptor extrae la clave pública del firmante del certificado y la utiliza para verificar la firma. La función de certificado digital proporciona a las entidades de IKE una forma escalable de autenticar la identidad de otra entidad de IKE.

Configuración de PKI

Esta versión asume que las dos entidades de IKE de una negociación utilizan la misma CA. Antes de empezar las negociaciones de IKE con su firma, deberá configurar PKI para el direccionador. También debe generar la clave privada y el certificado del direccionador, y debe haber bajado el certificado de la CA root. Los siguientes pasos explican cómo configurar la PKI:

1. Genere el par de claves y solicite el certificado.

   Puesto que la operación de claves públicas implica un par de claves (la modalidad de firma utiliza la clave privada para firmar y la clave pública para verificar), debe generar un par de claves para el direccionador. Para una solicitud de certificado, debe enviar la clave pública generada a la CA para ponerla en un certificado digital X.509. Luego, cada igual de IKE potencial podrá extraer su clave pública del certificado emitido por la CA. La clave privada reside en el direccionador y se mantiene en secreto, sólo la sabe el direccionador.

   En esta versión, puede emitir un mandato **certificate request** que hace lo siguiente:

   a. Genera un par de claves, cuya longitud puede especificar en 512, 768 o 1024 bits. La clave privada generada se mantiene en la antememoria.
   b. Solicita que entre información para incluir en la solicitud de certificado (por ejemplo, el ID del direccionador en forma de dirección IP, nombre de dominio o nombre de correo electrónico.
   c. Crea una solicitud de certificados (en formato PKCS#10) que contiene la clave pública generada y la información que ha entrado.
   d. Lleva a cabo un TFTP en la solicitud del certificado para una máquina de sistema principal.

2. Emita el certificado (fuera del direccionador)

   La CA recibe la solicitud de certificado de PKCS#10. La CA puede verificar manualmente la solicitud 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, que se convierte en información digital fiable siempre que se confíe en la CA que firma. El certificado ya está preparado para ser utilizado en las negociaciones de IKE. (Este proceso está fuera del ámbito del funcionamiento del direccionador y no se especifica más detalladamente en este manual.)

3. Baje el certificado del direccionador

   Cuando la CA haya emitido el certificado, la PKI puede bajarlo al direccionador. Según cómo la CA publique el certificado, la PKI puede utilizar TFTP o LDAP para bajarlo.

   Tenga en cuenta que la clave privada y la clave pública del certificado del direccionador deben coincidir para llevar a cabo el funcionamiento de clave pública como la firma digital. Cuando la PKI baja el certificado al direccionador, la clave privada que se ha generado con la clave pública debe estar en la antememoria clave del direccionador. El certificado bajado es inútil si pierde la clave privada que coincide. Esto significa que desde el momento en que se emite la solicitud de certificado al momento en que se baja el certificado **no debe** reiniciar o recargar el direccionador, borrar la antememoria o emitir una nueva solicitud de certificado. Cualquiera de estas operaciones destruirían la clave privada de la antememoria en ejecución del direccionador.

4. Baje el certificado de CA

   Para verificar el certificado del igual de IKE, PKI debe obtener el certificado de CA root. Esta versión da soporte a la operación de CA de un solo nivel, lo que significa que se deben asignar las entidades de IKE a la misma CA. Cada entidad de IKE (en este caso, cada direccionador) debe bajar el certificado de la CA (mediante TFPT o LDAP) para verificar que el certificado recibido del igual es válido.

5. Guarde y vuelva a cargar el certificado

   Cuando el direccionador ha obtenido el certificado, la clave privada coincidente y el certificado de la CA, puede empezar la negociación de IKE. Puesto que los certificados suelen ser válidos durante meses o años, es posible que quiera guardar el certificado y la clave privada en SRAM para que no tenga que emitir una solicitud de certificado y bajarlo cada vez que vuelva a cargar o reiniciar el direccionador. Esta versión proporciona los mandatos **cert save** y **cert load** para guardar o recuperar el certificado y la clave privada en SRAM.

   Tenga en cuenta que el certificado del direccionador y la clave privada se deben procesar como par (por ejemplo, siempre se deben guardar o recuperar conjuntamente de 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 siguientes ejemplos:

Ejemplo: Añadir servidor (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: Listar configuración de servidor (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: Listar certificados root (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 Usuage:   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 Usuage:   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 Usuage:   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 Usuage:   Sign & Encipherment
           Validity:   1998/10/29 -- 2001/10/29
       Default Cert:   No
```

Ejemplo: Solicitud de certificados (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: Listar certificados de direccionadores (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 Usuage:   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: Guardar certificado (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: Carga de certificados (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 IP manual (IPv4)

La función de seguridad de IP que se incluye en IPv4 para el 2212, junto con la función de política y otros procesos relacionados con IPSec, proporciona integridad de la autenticación, confidencialidad y no rechazamiento. Para implementar IPSec manualmente, preconfigure una política que contenga un subconjunto de opciones de IPSec en una base de datos de políticas para definir el período de validez y el perfil del túnel manual. También puede preconfigurar todo el conjunto de opciones de IPSec (política) de la base de datos para que cuando un direccionador habilitado para políticas se prepara para enviar un paquete de IPSec, negocie y establezca dinámicamente las opciones de IPSec con el direccionador de destino, según el contenido de la política. Para definir un túnel manual, consulte el apartado “Configuración de la seguridad IP manual (IPv4)” en la página 358. Para obtener una explicación de las opciones de política, consulte el Capítulo 18, “Utilización de la función de política” en la página 275.

Utilización de la seguridad de IP manual (IPv6)

La función de seguridad IP incluida en IPv6 para el 2212 proporciona autenticación, integridad y confidencialidad. Para definir un túnel manual, consulte el apartado “Configuración de la seguridad IP manual (IPv6)” en la página 369.

Capítulo 21. Configuración y supervisión de la seguridad IP

Este capítulo describe el modo de configurar y supervisar la seguridad IP y el modo de utilizar los mandatos de supervisión de la seguridad IP. Por lo que se refiere a IPv4, el Capítulo 18, "Utilización de la función de política" en la página 275 y el Capítulo 19, "Configuración y supervisión de la función de política" en la página 311 proporcionan información adicional sobre la configuración y supervisión de las políticas de seguridad IP. Este capítulo comprende las siguientes secciones:

- "Configuración del intercambio de claves en Internet (IPv4)"
- "Configuración de la infraestructura de claves públicas (IPv4)" en la página 354
- "Obtención de un certificado" en la página 354
- "Mandatos de configuración de la infraestructura de claves públicas" en la página 355
- "Configuración de la seguridad IP manual (IPv4)" en la página 358
- "Acceso al entorno de configuración de la seguridad IP" en la página 359
- "Mandatos de configuración de seguridad IP manual" en la página 359
- "Configuración de un túnel manual (IPv4)" en la página 368
- "Configuración de la seguridad IP manual (IPv6)" en la página 369
- "Acceso al entorno de configuración de la seguridad IP" en la página 370
- "Mandatos de configuración de seguridad IP manual" en la página 371
- "Configuración de un túnel manual (IPv6)" en la página 371
- "Supervisión de la seguridad IP manual (IPv4)" en la página 375
- "Supervisión de la seguridad IP manual (IPv6)" en la página 387

Nota: Si crea un túnel IPSec para transportar el tráfico de TN3270, APPN-ISR, o APPN-HPR y pretende dar prioridad a dicho tráfico mediante BRS, es necesario que utilice la función de establecimiento de bit de prioridad IPv4 de BRS. Consulte "Proceso de bits de precedencia de IP versión 4 para tráfico SNA en túneles seguros IP y fragmentos secundarios" en la página 10 si desea obtener más información.

Configuración del intercambio de claves en Internet (IPv4)

Este tema describe la manera de configurar el intercambio de claves en Internet (IKE).

Antes de establecer un túnel IPSec, deberá:

1. Configurar los atributos de paquetes que el túnel utilizará y las acciones resultantes que se deberán llevar a cabo (la política).
2. Configurar las opciones de cifrado y autenticación que desee.

Si desea obtener información detallada sobre cómo llevar a cabo dichas tareas, consulte el Capítulo 18, "Utilización de la función de política" en la página 275, Capítulo 19, "Configuración y supervisión de la función de política" en la página 311 y el "Configuración de la infraestructura de claves públicas (IPv4)" en la página 354.

Configuración de la infraestructura de claves públicas (IPv4)

Este tema describe la manera de configurar la infraestructura de claves públicas (PKI) con IPv4.

Antes de establecer un túnel IPSec, deberá:

1. Crear un par de claves de cifrado públicas/privadas y obtener un certificado digital de una Autoridad de certificación (CA) de confianza. Consulte "Obtención de un certificado" si desea obtener información detallada al respecto.
2. Decidir qué algoritmos IPSec, SA y demás opciones desea utilizar para los direccionadores cuyas políticas está configurando. Consulte "Negociación de un túnel de seguridad IP" en la página 346 y los temas posteriores para obtener información detallada.
3. Configurar el IKE y la base de datos de política. Consulte "Configuración del intercambio de claves en Internet (IPv4)" en la página 353, el Capítulo 18, "Utilización de la función de política" en la página 275 y el Capítulo 19, "Configuración y supervisión de la función de política" en la página 311 si desea obtener información detallada al respecto.

Obtención de un certificado

Antes de establecer un túnel IPSec, lo debe seleccionar y registrar con una Autoridad de certificación (CA) de confianza, tal y como se describe en "Utilización de la Infraestructura de claves públicas" en la página 347. La CA devuelve un certificado digital X.509 firmado que le permite identificarse y autenticarse ante terceros en la red. El certificado consiste en un ID digital codificado (firma) y un par de claves de cifrado públicas/privadas. Lleve a cabo lo siguiente:

1. Identifique una CA y obtenga su dirección de servidor.
2. Configure las opciones de recuperación de depósito mediante el mandato **add ldapserver** o el mandato **add tftpserver** de PKI Talk 6, tal y como se describe en "Mandatos de configuración de la infraestructura de claves públicas" en la página 355.
3. Cree un par de claves públicas/privadas mediante el mandato **certificate request** de PKI Talk 5, tal y como se describe en "Mandatos de supervisión de la infraestructura de claves públicas" en la página 378. Esto lo puede realizar tanto en el direccionador como remotamente, en calidad de administrador de la red privada virtual (VPN), en cuyo caso deberá cifrar y transferir de manera segura el par de claves al direccionador.
4. Envíe una petición de certificado inicial a la CA mediante el mandato **certificate request** de PKI Talk 5, tal y como se describe en "Mandatos de supervisión de la infraestructura de claves públicas" en la página 378. La petición se envía en un mensaje PKCS#10 vía correo electrónico o FTP. La CA vincula el par de claves al certificado, lo firma con su clave privada y lo almacena en un depósito central (LDAP o FTP) o se lo devuelve en un mensaje PKCS#7. Habitualmente, un certificado es válido durante varios meses o más, al cabo de los cuales se renueva. Con ello se identifican las partes de una red que aún son de confianza.
5. Guarde el certificado en una SRAM del direccionador mediante el mandato **certificate save** de PKI Talk 5, tal y como se describe en "Mandatos de supervisión de la infraestructura de claves públicas" en la página 378.

Notas:

1. Para visualizar una lista de los registros de certificados de la SRAM utilice el mandato **list certificate** de PKI Talk 6, tal y como se describe en "Mandatos de configuración de la infraestructura de claves públicas" en la página 355.
2. Para suprimir registros de certificados de la SRAM , utilice el mandato **delete certificate** de PKI Talk 6, tal y como se describe en "Mandatos de configuración de la infraestructura de claves públicas" en la página 355.
3. Para eliminar la necesidad de volver a enviar una petición de certificado durante futuras negociaciones de IPSec, utilice el mandato **certificate load** de PKI Talk 5, tal y como se describe en "Mandatos de supervisión de la infraestructura de claves públicas" en la página 378 para cargar el certificado recibido en la antememoria.

Mandatos de configuración de la infraestructura de claves públicas

Add

Utilice el mandato **add** de PKI Talk 6 para configurar el servidor de depósitos de certificados y su ubicación.

Sintaxis:

a**dd** server

server Especifica que la operación de adición se aplica 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 **change** de PKI Talk 6 para cambiar el servidor de depósitos de certificados y su ubicación.

Sintaxis:

c**hange**
server

server Especifica que la operación de cambio se aplica a un servidor.

Ejemplo 1: Cambio de un servidor

```
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 **delete** de PKI Talk 6 para suprimir un registro de certificados o un registro de claves privadas de una SRAM del direccionador o para suprimir un servidor.

Sintaxis:

d**elete**
certificate
private-key
server

certificate
Especifica que la operación de supresión se aplica a uno o más registros de certificados.

all Especifica que se deben suprimir todos los registros de certificados.

id Especifica el ID del registro del certificado a suprimir.

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 de servidor

```
PKI config>delete server
Name []? myldap
Server MYLDAP deleted successfully
```

private-key
Especifica que la operación de supresión se aplica a uno o más registros de claves privadas.

server Especifica que la operación de supresión se aplica a un servidor.

List

Utilice el mandato **list** de PKI Talk 6 para listar los registros de certificados o claves en una SRAM del direccionador.

Sintaxis:

list certificates
private-keys
servers

certificates
Especifica que la operación de listado se aplica a los registros de certificados.

private-keys
Especifica que la operación de listado se aplica a los registros de claves privadas.

servers
Especifica que la operación de listado se aplica a los registros de servidor.

Ejemplo 1: Listado de 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 Usuage:   Sign & Encipherment
           Validity:   1999/1/19 23:24:27 -- 2002/1/19 23:54:27
       Default Cert:   No
```

Ejemplo 2: Listado de claves privadas

```
PKI config>list private-keys
Private Keys In SRAM:

1) Name W
```

Ejemplo 3: Listado de 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 IP manual (IPv4)

Esta sección describe las opciones de configuración disponibles para la IPSec manual con IPv4. Todas las funciones IPSec se aplican a IPv4.

Lleve a cabo los siguientes pasos para configurar un túnel manual IPSec:

1. Cree el túnel IPSec.
2. Restablezca IPSec.
3. Configure la política del túnel manual (perfil, validez, política).
4. Restablezca la política.

Configuración de los algoritmos

Puede configurar políticas de túnel con los algoritmos que aparecen en la Tabla 41.

Tabla 41. Algoritmos configurados con varias políticas de túneles

Política de túnel	Algoritmos
AH, AH-ESP o ESP-AH	• Algoritmo de autenticación AH local—Obligatorio • Algoritmo de autenticación AH remota—Opcional
ESP, AH-ESP o ESP-AH	• Algoritmo de cifrado local—Obligatorio • Algoritmo de cifrado remoto—Opcional • Algoritmo de autenticación ESP local—Opcional • Algoritmo de autenticación ESP remota—Opcional **Nota:** Si su carga de software no incorpora cifrado, no verá los parámetros relacionados con el cifrado.

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 del direccionador que se encuentra en el extremo más cercano de un túnel debe coincidir con el algoritmo remoto del direccionador que se encuentra 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 es opcional.

Configuración de las claves de cifrado

Para cada algoritmo local que configure debe configurar también una clave que sea idéntica a la clave del algoritmo correspondiente en el sistema principal remoto. Consulte la descripción de las claves del mandato **add tunnel** en "Mandatos de configuración de seguridad IP manual".

Acceso al entorno de configuración de la seguridad IP

Para acceder al entorno de configuración de la seguridad 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 configuración de seguridad IP manual

Esta sección describe los mandatos de configuración de la seguridad IP. Entre estos mandatos en el indicador IPV4-IPsec config>.

Tabla 42. Resumen de mandatos de configuración de seguridad IP

Mandato	Función
? (Ayuda)	Visualiza todos los mandatos disponibles para este nivel de mandato, o lista las opciones de mandatos específicos (si es que están disponibles). Consulte "Obtención de ayuda" en la página xxv.
Add tunnel	Añade un túnel seguro.
Change tunnel	Cambia los valores de los parámetros de configuración de un túnel seguro.
Delete tunnel	Suprime un túnel seguro.
Disable	Inhabilita todo el proceso de seguridad IP de manera segura (se eliminan los paquetes que coinciden con los filtros de paquete), inhabilita todo el proceso de seguridad IP de manera no segura (se aceptan los paquetes que coinciden con los filtros de paquete) o inhabilita un túnel seguro.
Enable	Habilita todo el proceso de seguridad IP o inhabilita un túnel seguro.
List	Lista información global sobre la seguridad IP o información sobre túneles definidos.
Set	Establece varias opciones de IPSec.
Exit	Hace volver al nivel de mandato anterior. Consulte "Salida de un entorno de nivel inferior" en la página xxv.

Add Tunnel

Utilice el mandato **add tunnel** para añadir los parámetros necesarios para definir un túnel IPSec.

Sintaxis:

add tunnel...

Mandatos de configuración de seguridad IP manual

nombre del túnel
Parámetro opcional para etiquetar el túnel. Debe ser exclusivo dentro del 2212.

Valores válidos: hasta 15 caracteres; el primer carácter tiene que ser una letra; no se pueden dejar espacios en blanco.

Valor por omisión: ninguno

tiempo de vida
El tiempo en minutos durante el que el túnel puede estar activo. El valor 0 indica que el túnel no caduca nunca.

Valores válidos: 0 - 525600 (0 = no caduca; 525600 = 365 días)

Valor por omisión: 46080 (32 días)

modalidad de encapsulación
La manera como está encapsulado el paquete IP. En modalidad de túnel, todo el paquete IP se encapsula y se crea una nueva cabecera IP; en modalidad de transporte, la cabecera IP no se encapsula. Si uno de los extremos del túnel seguro es un direccionador, se ***debe*** utilizar, pues, la modalidad de túnel, de acuerdo con el borrador de arquitectura de seguridad del equipo negociador de ingeniería de internet (IETF).

Valores válidos: tunnel (*TUNN*) o translate (*TRANS*)

Valor por omisión: tunnel (*TUNN*)

política del túnel
Una de las cuatro opciones que definen la política de túnel: cabecera de autenticación (AH) de IP, carga útil de seguridad de encapsulación (ESP) de IP o combinaciones de dichos protocolos (AH-ESP y ESP-AH). En AH-ESP, el cifrado de ESP se ejecuta primero en los paquetes de salida; en ESP-AH, la autenticación AH se ejecuta en primer lugar en los paquetes de salida. Algunos parámetros son exclusivos de ESP o AH. Los parámetros de cifrado se configuran sólo si ESP, AH-ESP o ESP-AH está seleccionado; los parámetros de autenticación se configuran sólo si AH, AH-ESP o ESP con autenticación está seleccionado.

Valores válidos: AH, ESP, AH-ESP, ESP-AH

Valor por omisión: AH-ESP

dirección IP local
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 2212.

Valor por omisión: una de las direcciones IP configuradas para el direccionador

spi local
Una asociación de seguridad es una conexión de seguridad unidireccional que utiliza AH o ESP para proteger el tráfico de conexión. El índice de parámetros de seguridad (SPI) es un valor de 32 bits arbitrario que identifica exclusivamente una de las dos asociaciones de seguridad (entrada o salida) asociadas con este túnel seguro. Este parámetro, que es obligatorio, identifica el SPI esperado en este túnel para paquetes de entrada recibidos en el extremo local del túnel. Este valor no puede coincidir con el SPI local de otro túnel que disponga de la misma dirección local de IP. Independientemente de

la política de túnel (ESP, AH, AH-ESP o ESP-AH), sólo se configura un SPI local para el tráfico de entrada de un túnel seguro de IP.

Valores válidos: cualquier valor de 32 bits mayor de 255

Valor por omisión: 256

algoritmo de cifrado local
El algoritmo de cifrado utilizado para ESP en paquetes de salida enviados desde el direccionador local, que es obligatorio para la configuración de ESP. En algunos países, es probable que algunos o todos estos algoritmos no estén disponibles debido a las normas de exportación de los EE.UU. Este algoritmo de cifrado debe coincidir con el algoritmo de cifrado remoto.

El algoritmo ESP-NULL evita que ESP lleve a cabo un cifrado. Este algoritmo está disponible en todos los países. Si se selecciona ESP-NULL, ESP debe activarse para 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

clave de cifrado local
La clave o claves utilizadas 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 está configurada cuando el algoritmo de cifrado ESP-NULL está seleccionado.

Valores válidos:

- Para DES-CBC: 16 caracteres hex (0 - 9, a - f, A - F)
- Para CDMF: 16 caracteres hex (0 - 9, a - f, A - F)
- Para 3DES: tres claves independientes, sin que se repita ninguna, teniendo cada una 16 caracteres hex (0 - 9, a - f, A - F)

Valor por omisión: ninguno

relleno para cifrado local
Tamaño en bytes de relleno adicional que se añade a los paquetes ESP de salida. El relleno adicional se puede utilizar para disfrazar el tamaño de los paquetes IP que se están cifrando cuando el algoritmo de cifrado da como resultado un paquete cifrado que es del mismo tamaño que el paquete original. Los valores de relleno ESP deben ser múltiplos de 8. Si se configura un valor que no es divisible por 8, dicho valor se redondea a la alza hasta el siguiente valor que sí que es divisible por 8.

Cuando el algoritmo de cifrado es ESP-NULL, el relleno no es necesario porque el algoritmo ESP-NULL añade un byte al tamaño del paquete original. Si se configura relleno para cifrado local, el valor es ignorado.

Valores válidos: 0 - 120

Valor por omisión: 0

autenticación ESP local
Selecciona autenticación ESP local, si se desea. La autenticación es obligatoria si el algoritmo de cifrado es ESP-NULL.

Valores válidos: Yes (Sí) o No

Valor por omisión: Yes (Sí)

Mandatos de configuración de seguridad IP manual

algoritmo de autenticación local

Algoritmo de autenticación que se utiliza en los paquetes de salida. Es un parámetro opcional para ESP y no será obligatorio a no ser 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 extremo más alejado del túnel IPSec.

Valores válidos: HMAC-MD5 o HMAC-SHA

Valor por omisión: HMAC-MD5

clave de autenticación local

Clave utilizada con el algoritmo de autenticación local. Debe coincidir con la clave equivalente que está configurada en el extremo opuesto del túnel IPSec. Es obligatorio 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 hex (0 - 9, a - f, A - F)
- para HMAC-SHA: 40 caracteres hex (0 - 9, a -f, A - F)

Valor por omisión: ninguno

dirección IP remota

Dirección IP para el extremo remoto del túnel. Es un parámetro obligatorio.

Valores válidos: una dirección IP válida

Valor por omisión: ninguno

spi remoto

Una asociación de seguridad es una conexión de seguridad de unidireccional que utiliza AH o ESP para proteger el tráfico de conexión. El índice de parámetros de seguridad (SPI) es un valor de 32 bits arbitrario que identifica exclusivamente una de las dos asociaciones de seguridad (entrada o salida) asociadas con este túnel seguro. Este parámetro, que es obligatorio, identifica el SPI esperado en ESP o AH para paquetes de salida destinados para el sistema principal remoto. Este valor no puede coincidir con el SPI remoto de otro túnel que disponga de la misma dirección remota de IP. Independientemente de la política de túnel (ESP, AH, AH-ESP, or ESP-AH), sólo se configura un SPI local para tráfico de salida para un túnel IPSec.

Valores válidos: cualquier valor de 32 bits mayor de 255

Valor por omisión: 256

algoritmo de cifrado remoto

Algoritmo de descifrado utilizado en paquetes de entrada recibidos desde el sistema principal remoto. Debe coincidir con el algoritmo de cifrado local.

El algoritmo ESP-NULL evita que ESP lleve a cabo un cifrado. Si se selecciona ESP-NULL, ESP debe activarse para 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

clave de cifrado remoto

Clave o claves utilizadas con el algoritmo de cifrado ESP remoto. Deben coincidir con las claves equivalentes que están configuradas en el extremo

opuesto del túnel seguro. Esta clave no está configurada cuando el algoritmo de cifrado ESP-NULL está seleccionado.

Valores válidos:

- Para DES-CBC: 16 caracteres hex (0 - 9, a - f, A - F)
- Para CDMF: 16 caracteres hex (0 - 9, a - f, A - F)
- Para 3DES: tres claves independientes, sin que coincida ninguna, teniendo 16 caracteres en hex (0 - 9, a - f, A - F)

Valor por omisión: ninguno

verificación del relleno de cifrado remoto
Determina si el tamaño del relleno del cifrado de los paquetes recibidos debe ser verificado.

Valores válidos: Yes (Sí) o No

Valor por omisión: No

relleno para cifrado remoto
Tamaño en bytes de relleno adicional que se espera en los paquetes ESP recibidos. Este parámetro es obligatorio y válido si el valor *verification-of-remote-encryption-padding* es Yes (Sí). Los valores de relleno deben ser múltiplos de 8. Si se configura un valor que no es divisible por 8, dicho valor se redondeará al alza hasta el siguiente valor que sí que sea divisible por 8.

Valores válidos: 0 - 120

Valor por omisión: 0

autenticación ESP remota
Selecciona la autenticación ESP remota para paquetes de entrada, si se desea.

Valores válidos: Yes (Sí) o No

Valor por omisión: Yes (Sí)

algoritmo de cifrado remoto
Algoritmo de autenticación utilizado para paquetes de entrada. Es un parámetro opcional para ESP y no será obligatorio a no ser que se seleccione la autenticación ESP. Este parámetro es obligatorio para AH o combinaciones de AH y ESP (AH-ESP o ESP-AH). El algoritmo de autenticación utilizado debe coincidir con el algoritmo de autenticación local utilizado en el extremo más alejado del túnel IPSec.

Valores válidos: HMAC-MD5 o HMAC-SHA

Valor por omisión: HMAC-MD5

clave de autenticación remota
Clave utilizada con el algoritmo de autenticación remota. Debe coincidir con la clave equivalente que está configurada en el extremo opuesto del túnel seguro. Es obligatorio en AH, AH-ESP y ESP-AH y en ESP si el algoritmo de autenticación ESP remota se ha configurado.

Valores válidos:

- para HMAC-MD5: 32 caracteres hex (0 - 9, a - f, A - F)
- para HMAC-SHA: 40 caracteres hex (0 - 9, a -f, A - F)

Valor por omisión: ninguno

habilitar prevención de reproducción
Especifica si la prevención de reproducción está habilitada o no. Si la prevención de reproducción está habilitada, los números de secuencia de las cabeceras de seguridad IP se supervisan para evitar que el túnel receptor procese paquetes duplicados. No se recomienda utilizar la prevención de reproducción porque la asociación de seguridad de túnel debe estar desactivada cuando el contador de números de secuencia del emisor alcanza el límite. Cuando ello sucede, es necesaria una intervención manual para reiniciar la asociación de seguridad existente o crear una nueva.

Así mismo, si la prevención de reproducción está habilitada y se reinicia IPSec mediante el mandato **reset ipsec**, debe asegurarse de que IPSec también se reinicia en el direccionador que se encuentra en el otro extremo del túnel IPSec. Ello es necesario para reinicializar el número de secuencias en los dos extremos del túnel. Si IPSec se reinicia en un extremo del túnel y en el otro no, es posible que los direccionadores que se encuentran en cada uno de los extremos del túnel eliminen paquetes a causa de la discrepancia de números de secuencia.

Valores válidos: Yes (Sí) o No

Valor por omisión: No

bit DF
Especifica el manejo del bit No fragmentar (DF) en la cabecera externa para túneles seguros de modalidad de túnel. Se puede establecer este bit en cabeceras IPv4 para especificar que el paquete no se puede fragmentar. El parámetro DF-bit indica al 2212 cómo debe manejar el bit en paquetes entrantes - ya sea copiando en la cabecera externa el valor del DF-bit hallado en la cabecera interna, o estableciendo o borrando el bit en la cabecera externa.

Si se establece el bit DF y el paquete no se puede fragmentar, IPSec utiliza la función Path MTU (PMTU) Discovery. Consulte “Descubrimiento de la unidad de transmisión máxima de la vía de acceso” en la página 343 si desea obtener más información.

Valores válidos: Copy, Set, Clear

Valor por omisión: Copy

habilitar túnel
Especifica si el túnel está habilitado. El túnel habilitado no filtrará paquetes hasta que se haya configurado un filtro de paquete para definir la interfaz sobre la que este túnel IPSec operará y hasta que IP se haya restablecido o reiniciado en el 2212. Puede utilizar el mandato **reset ip** para restablecer IP.

Valores válidos: Yes (Sí) o No

Valor por omisión: Yes (Sí)

Change Tunnel

Utilice el mandato **change tunnel** para cambiar un parámetro de túnel IPSec que se haya configurado anteriormente mediante el mandato **add tunnel**.

Sintaxis:

change tunnel...
Consulte el mandato **add tunnel** para obtener una lista de los parámetros que se pueden cambiar.

Delete Tunnel

Utilice el mandato **delete tunnel** de Talk 6 para suprimir un túnel IPSec.

Sintaxis:

de**lete** t**unnel**
id de túnel
nombre de túnel
all

id de túnel
Especifica el identificador del túnel IPSec que se debe suprimir.

Valores válidos: 1 - 65535

Valor por omisión: 1

nombre de túnel
Especifica el nombre del túnel IPSec que se debe suprimir.

Valores válidos: cualquier nombre de túnel configurado

Valor por omisión: ninguno

all Especifica que todos los túneles IPSec de esta interfaz deben ser suprimidos.

Disable

Utilice el mandato **disable** para inhabilitar el túnel IPSec o para inhabilitar todos los túneles IPSec ya sea de manera segura (los paquetes que coinciden con los filtros IPSec se eliminan), ya sea de manera insegura (se aceptan los paquetes que coinciden con los filtros IPSec).

Sintaxis:

di**sable**
ipsec drop
ipsec pass
tunnel ...

ipsec drop
Inhabilita la seguridad IP en el direccionador de manera segura. Todos los túneles IPSec se inhabilitarán pero la información de túnel seguro de las normas de filtro de paquetes se utiliza para identificar los paquetes que coinciden con los filtros de paquetes de túnel IPSec. Los paquetes coincidentes se eliminan.

ipsec pass
Inhabilita la seguridad IP en el direccionador de manera no segura. Se inhabilitarán todos los túneles IPSec. Los paquetes que coinciden con los filtros de paquetes de túnel se reenvían como tráfico ordinario.

tunnel *id-túnel nombre-túnel* **all**
Inhabilita la seguridad IP en un túnel especificado o en todos los túneles.

id de túnel
Especifica el identificador del túnel seguro que se debe inhabilitar.

Valores válidos: 1 - 65535

Valor por omisión: 1

nombre de túnel
Especifica el nombre del túnel seguro que se debe 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 IP en todas las interfaces o en un único túnel. Debe habilitar IPSec de manera global en el direccionador antes de que los túneles IPSec habilitados de manera individual se activen.

Sintaxis:

enable
ipsec
tunnel ...

ipsec
Habilita la seguridad IP a través del direccionador.

tunnel *id-túnel nombre-túnel* **all**
Habilita la seguridad IP en un túnel especificado o en todos los túneles.

id de túnel
Especifica el identificador del túnel seguro que se debe habilitar.

Valores válidos: 1 - 65535

Valor por omisión: 1

nombre de túnel
Especifica el nombre del túnel seguro que se debe 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 de seguridad IP actual. Los túneles globales incluyen todos los túneles del direccionador, tanto activos como definidos. Todos los túneles incluyen todos los túneles configurados en esta interfaz, tanto activos como definidos. Los túneles activos son los que están activos en este momento; los túneles definidos son los que están definidos pero no están activos. Para IPv4, también se listan los certificados seleccionados en una SRAM de direccionador.

Sintaxis:

list ...
all
status
tunnel
active *id-túnel nombre-túnel* all
defined *id-túnel nombre-túnel* all

Ejemplo 1: Listado de todos los túneles 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      *****************
```

Ejemplo 2: Listado de un túnel IPSec con la política ESP y el algoritmo ESP-NULL

```
IPsec config>li tun 1000

Tunnel  Name             Mode   Policy   Life   Replay  Rcv  IPsec  State
ID                                              Prev    Win  Vers
------  ---------------  -----  ------  ------  ------  ---  -----  --------
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 PMTU del túnel.

Sintaxis:

set path-mtu-age-timer

path-mtu-age-timer
Especifica el tiempo (en minutos) que transcurrirá antes de que el 2212 restaure el valor PMTU del túnel al valor máximo.

Valor por omisión: 10 (0 significa inhabilitado)

Configuración de un túnel manual (IPv4)

Este tema proporciona información sobre la configuración de un túnel manual IPv4 para la red que aparece en la Figura 37 en la página 344.

Configuración del túnel para el direccionador A

El siguiente ejemplo muestra la manera de configurar un túnel manual IPSec para el direccionador A en la red que aparece en la Figura 37 en la página 344 mediante 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 comprobar en este ejemplo, se le solicitan los parámetros que es necesario especificar. La configuración de un túnel ESP, AH-ESP o ESP-AH solicita parámetros similares.

Nota: Los valores de las claves no se visualizan al entrarlos. Por lo tanto, no son visibles en el ejemplo. Si las claves de la autenticación HMAC-MD5 fueran visibles, se verían 32 caracteres hexadecimales. Por ejemplo, una clave puede tener el valor: X' 1234567890ABCDEF1234567890ABCDEF'.

Configuración del túnel para el direccionador B

Debe configurar dentro del direccionador B el mismo túnel manual IPSec que se haya configurado para el direccionador A, túnel 1 IPSec. 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 IPSec deben coincidir con los parámetros que se han configurado para el direccionador A.

Ejemplo: Configuración manual de un túnel de seguridad IP con ESP

Observe que se le solicita que establezca el bit DF cuando el túnel está en modalidad de túnel y la política de túnel es ESP. Este ejemplo muestra sólo la configuración del túnel IPSec, no de los filtros de paquetes.

```
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 IP con ESP y ESP-NULL

Observe que la autenticación es obligatoria.

```
IPV4-IPsec config>add tunnel
Adding tunnel 3
Tunnel Name (optional)? tunnel3
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 IP manual (IPv6)

Esta sección describe las opciones de configuración disponibles para IPSec manual con IPv6. Todas las funciones IPSec se aplican a IPv6. Observe los siguientes cambios en las preguntas de configuración IPSec al configurar IPSec para IPv6:

- Entre las direcciones en el formato de direcciones IPv6 (por ejemplo, 8:0:9:8::1).
- No se le solicita que establezca el bit DF.

Lleve a cabo los siguientes pasos para configurar un túnel manual IPSec:

1. Cree el túnel IPSec.

2. Restablezca IPSec.
3. Configure las normas de filtro.
4. Restablezca IPV6.

Configuración de los algoritmos

Puede configurar políticas de túnel con los algoritmos que aparecen en la Tabla 43.

Tabla 43. Algoritmos configurados con varias políticas de túneles

Política de túnel	Algoritmos
AH, AH-ESP o ESP-AH	• Algoritmo de autenticación AH local—Obligatorio • Algoritmo de autenticación AH remota—Opcional
ESP, AH-ESP, or ESP-AH	• Algoritmo de cifrado local—Obligatorio • Algoritmo de cifrado remoto—Opcional • Algoritmo de autenticación ESP local—Opcional • Algoritmo de autenticación ESP remota—Opcional **Nota:** Si su carga de software no incorpora cifrado, no verá los parámetros relacionados con el cifrado.

Una política de túnel utiliza un algoritmo local en paquetes de salida y un algoritmo remoto en paquetes de salida. El algoritmo local del direccionador que se encuentra en el extremo más cercano de un túnel debe coincidir con el algoritmo remoto del direccionador que se encuentra 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 es opcional.

Configuración de las claves de cifrado

Para cada algoritmo que configure debe configurar también una clave que sea idéntica a la clave del algoritmo correspondiente en el sistema principal remoto. Consulte la descripción de las claves del mandato **add tunnel** en “Mandatos de configuración de seguridad IP manual” en la página 359.

Acceso al entorno de configuración de la seguridad IP

Para acceder al entorno de configuración de la seguridad 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>ipv6
IPV6-IPsec config>
```

Mandatos de configuración de seguridad IP manual

Consulte “Mandatos de configuración de seguridad IP manual” en la página 359 si desea obtener una descripción de los mandatos de configuración de seguridad IP disponibles para IPv6. Los mandatos para 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 en la Figura 37 en la página 344 mientras lee este tema. El túnel 1 IPSec dispone de un punto final en la interfaz 1 del direccionador A. El direccionador A se configurará para IPSec. Lleve a cabo los siguientes pasos para configurar un direccionador A manualmente:

1. Cree el túnel IPSec.
2. Cree un filtro de paquetes de salida en la interfaz del direccionador que sea el punto final del túnel IPSec.
3. Cree reglas de control de acceso para los filtros de paquetes.
4. Restablezca IPSec.
5. Restablezca IPv6.

Creación del túnel de seguridad IP para el direccionador A

El siguiente ejemplo muestra la manera de crear el túnel 1 IPSec 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 comprobar en este ejemplo, se le solicitan los parámetros que es necesario especificar. La configuración de un túnel ESP, AH-ESP o ESP-AH solicita parámetros similares.

Nota: Los valores de las claves no se visualizan al entrarlos. Por lo tanto, no son visibles en el ejemplo. Si las claves de la autenticación HMAC-MD5 fueran visibles, vería 32 caracteres hex. Por ejemplo, una clave puede tener un valor X'1234567890ABCDEF1234567890ABCDEF'.

Configuración de filtros de paquetes para el direccionador A

Después de haber creado el túnel IPSec para el direccionador A, debe definir un filtro de paquetes IP. La creación del filtro de paquetes *out-router-A* aparece en el siguiente ejemplo. Consulte las secciones IPv6 Filtering y Access Control del capítulo Using IPv6 de la publicación *Configuración y supervisión de protocolos - Manual de consulta Volumen 1* si desea obtener más información sobre la configuración de filtros de paquetes IPv6 y normas de control de acceso.

```
*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 normas del control de acceso de filtros de paquetes para el direccionador A

El siguiente paso es la configuración de las normas de control de acceso de filtros de paquetes. Cree dos normas de control de acceso en el filtro de paquetes de salida *out-router-A*.

Las normas de control de acceso del filtro de paquetes de salida llevan a cabo las siguientes funciones:

- Una de las reglas de control de acceso define el rango de las direcciones fuente y destino de los paquetes que deben pasar al túnel IPSec.
- La otra norma de control de acceso permite que el tráfico IPSec pase a través del filtro de paquetes.

Configure la primera norma de control de acceso para el filtro de paquetes *out-router-A*. Esta norma de control de acceso pasa paquetes desde la red 1000:1:: a la red de destino 3000:1:: 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 norma de control de acceso para *out-router-A* permite que los paquetes seguros pasen entre los dos extremos del túnel IPSec.

```
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 ocurre con los demás filtros de paquetes, es probable que desee configurar una norma de control de acceso comodín para que *out-router-A* pase tráfico que no coincida con ninguna de las normas de control de acceso.

Restablecimiento de la seguridad IP y de IP en el direccionador A

Después de que acabe de configurar la política, utilice el mandato **reset ipsec** de Talk 5 para volver a cargar la SRAM con la nueva configuración IPSec. El mandato **reset ipsec** no afecta a ninguna configuración IP. A continuación, utilice el mandato **reset ipv6** de Talk 5 para restablecer de manera dinámica IPv6 dentro del direccionador. Como alternativa, también puede reiniciar el direccionador para restablecer cada componente. Puede restablecer IPSec y IPv6 o reiniciar el direccionador para garantizar que las normas de filtro se vuelven a cargar. De lo contrario, es probable que la configuración no reciba el soporte adecuado en la interfaz. Consulte el Capítulo 21, "Configuración y supervisión de la seguridad IP" en la página 353 y el mandato **reset ipv6** de la publicación *Configuración y supervisión de protocolos - Manual de consulta Volumen 2* si desea obtener más información.

Tal y como aparece en la Figura 37 en la página 344, el túnel 2 IPSec dispone de un punto final en la interfaz 1 del direccionador B. Lleve a cabo los siguientes pasos para configurar el direccionador B manualmente.

1. Cree el túnel IPSec.
2. Cree un filtro de salida en la interfaz del direccionador que sea el el punto final del túnel IPSec.
3. Cree reglas de control de acceso para los filtros de paquetes.
4. Restablezca IPSec.
5. Restablezca IPv6.

Creación del túnel de seguridad IP para el direccionador B

Dentro del direccionador B, se debe crear el mismo túnel IPSec, túnel 2 de IPSec, que se ha creado para el direccionador A. 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 de túnel IPSec deben coincidir con los parámetros que se han especificado para el direccionador A.

Configuración de filtros de paquetes para el direccionador B

Tal y 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 punto final del túnel 1 de IPSec.

Configuración de las normas de control de acceso del filtro de paquetes para el direccionador B

Configure una norma de control de acceso en *out-router-B* para pasar paquetes de salida desde la red 3000:1:: a IPSec para proceso y transmisión a través del túnel 2 de IPSec. Esta norma de control de acceso es del 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>
```

Ahora cree para *out-router-B*, una norma de control de acceso inclusiva que permita que los paquetes que IPSec ha procesado pasen a través del túnel 2 IPSec.

```
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 norma de control de acceso comodín inclusiva si desea aceptar, en lugar de eliminar, los paquetes que no coinciden con una de las dos normas de control de acceso, por ejemplo, tráfico no destinado al túnel 2 de IPSec.

Restablecimiento de la seguridad IP y de IPv6 en el direccionador B

Antes de que la función IPSec funcione y de que se activen los filtros, debe restablecer IPSec e IPv6. Utilice el mandato **reset IPSec** de Talk 5 para restablecer IPSec e IPv6. Consulte “Restablecimiento de la seguridad IP y de IP en el direccionador A” en la página 373 si desea obtener más información sobre el restablecimiento de IPSec. Después de restablecer IPSec, utilice el mandato **reset IPv6** de Talk 5 para reiniciar IPv6. Como alternativa, también puede reiniciar el direccionador para restablecer cada componente.

Ejemplo: Configuración de un túnel de seguridad IP con ESP

Observe que este ejemplo muestra sólo la configuración del túnel IPSec, no la de los filtros de paquetes.

```
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 IP con ESP y ESP-NULL

Observe 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 IP manual (IPv4)

Esta sección explica la manera de supervisar IPSec manual con IPv4. Describe la manera de acceder al entorno intercambio de claves en Internet y los mandatos disponibles.

Acceso al entorno intercambio de claves en Internet

Esta sección explica la manera de utilizar el protocolo intercambio de claves en Internet (IKE) con IPv4.

Para acceder al entorno de supervisión de IKE de la seguridad IP, entre la secuencia de mandatos siguiente en el indicador +:

```
+ feature ipsec
IPSP>ike
IKE>
```

Mandatos de supervisión de intercambio de claves en Internet

Esta sección describe los mandatos de supervisión de IKE.

Tabla 44 (Página 1 de 2). Resumen de los mandatos de supervisión de IKE

Mandato	Función
? (Ayuda)	Visualiza todos los mandatos disponibles para este nivel de mandato, o lista las opciones de mandatos específicos (si es que están disponibles). Consulte “Obtención de ayuda” en la página xxv.

Tabla 44 (Página 2 de 2). Resumen de los mandatos de supervisión de IKE

Mandato	Función
Delete	Suprime de manera dinámica un SA de Fase 1 ISAKMP de un túnel específico o todos los SA de Fase 1.
List	Lista información sobre un SA de Fase 1 de un túnel específico o de todos los SA de Fase 1.
Stats	Visualiza las estadísticas de un túnel.
Exit	Hace volver al nivel de mandato anterior. Consulte “Salida de un entorno de nivel inferior” en la página xxv.

Delete

Utilice el mandato **delete** de IKE para suprimir de manera dinámica un SA de Fase 1 de un túnel o todos los SA de Fase 1.

Sintaxis:

delete
tunnel
all

tunnel Especifica que se debe suprimir un SA de Fase 1 para un túnel específico.

all Especifica que se deben suprimir todos los SA de Fase 1.

Ejemplo: Supresión de un túnel

```
PKI config>delete tunnel
Peer address [10.0.0.3]?
```

List

Utilice el mandato **list** de IKE para visualizar información sobre un SA de Fase 1 de un túnel específico o sobre todos los SA.

Sintaxis:

list tunnel
all

tunnel Especifica que se debe visualizar información de SA de un túnel específico.

all Especifica que se debe visualizar información de todos los SA.

Ejemplo: Listado de información de todos los 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 **stats** de IKE para visualizar estadísticas de túnel.

Sintaxis:

stats
tunnel

túnel Visualiza información estadística sobre los SA de un túnel.

Valores válidos: cualquier nombre de túnel o id de túnel.

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                0
```

Acceso al entorno de la infraestructura de claves públicas (IPv4)

Esta sección explica la manera de utilizar la infraestructura de claves públicas (PKI) con IPv4.

Mandatos de supervisión de PKI (talk 5)

Para acceder al entorno de supervisión de PKI de la seguridad IP, entre la siguiente secuencia de mandatos en el indicador +:

```
+ feature ipsec
IPSP>pki
PKI>
```

Mandatos de supervisión de la infraestructura de claves públicas

Esta sección describe los mandatos de supervisión de la infraestructura de claves públicas (PKI).

Tabla 45. Resumen de los mandatos de supervisión de PKI

Mandato	Función
? (Ayuda)	Visualiza todos los mandatos disponibles para este nivel de mandato, o lista las opciones de mandatos específicos (si es que están disponibles). Consulte “Obtención de ayuda” en la página xxv.
Cert-load	Carga un certificado en la SRAM de un direccionador.
Cert-req	Envía una petición de certificado a una CA.
Cert-save	Guarda un certificado en la antememoria para su posible uso futuro.
List certificate	Lista información sobre un certificado.
List configured-servers	Visualiza información sobre los servidores configurados.
Load certificate	Carga un registro que contiene el certificado de SRAM en la antememoria en tiempo de ejecución.
Exit	Hace volver al nivel de mandato anterior. Consulte “Salida de un entorno de nivel inferior” en la página xxv.

Cert-load

Utilice el mandato de PKI **cert-load** para cargar un registro que contenga el certificado y la clave privada de SRAM en la antememoria de certificados en tiempo de ejecución.

Sintaxis:

cert-load

Ejemplo: Carga de un registro de certificado de SRAM a 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 **cert-req** de PKI para solicitar un certificado de una CA.

Sintaxis:

cert-req

Ejemplo: Petición de un certificado de 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 **cert-save** de PKI para guardar un registro que contenga el certificado y la clave privada en la SRAM.

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 **list certificate** de PKI para visualizar información sobre un certificado digital X.509.

Sintaxis:

list certificate

Ejemplo: Listado 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 Usuage:   Sign & Encipherment
           Validity:   1999/1/19 23:24:27 -- 2002/1/19 23:54:27
```

List Configured-servers

Utilice el mandato **list configured-servers** para visualizar información sobre los servidores configurados.

Sintaxis:

list configured-servers

Ejemplo: Listado de información sobre 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 **load certificate** de PKI para cargar un certificado de SRAM a la antememoria en tiempo de ejecución.

Sintaxis:

load certificate

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 IP (IPv4)

Para acceder al entorno de supervisión de la seguridad IP de 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 IP (IPv4)

Esta sección describe los mandatos de supervisión de la seguridad IP.

Tabla 46. Resumen de mandatos de supervisión de la seguridad IP

Mandato	Función
? (Ayuda)	Visualiza todos los mandatos disponibles para este nivel de mandato, o lista las opciones de mandatos específicos (si es que están disponibles). Consulte “Obtención de ayuda” en la página xxv.
Change tunnel	Cambia de manera dinámica los valores de los parámetros de configuración de un túnel seguro.
Delete tunnel	Suprime de manera dinámica un túnel seguro.
Disable	Inhabilita de manera dinámica todo el proceso de seguridad IP de manera segura (los paquetes coincidentes se eliminan), inhabilita todo el proceso de seguridad IP de manera no segura (se reenvían los paquetes coincidentes) o inhabilita un túnel seguro concreto.
Enable	Habilita de manera dinámica todo el proceso de seguridad IP o habilita un túnel seguro.
List	Lista información global sobre la seguridad IP y sobre túneles activos y definidos.
Reset	Restablece la seguridad IP o restablece un túnel seguro. Este mandato vuelve a cargar la configuración que se ha creado en Talk 6. Al restablecer se alterarán temporalmente los valores de los parámetros configurados mediante Talk 5 por los que se hayan configurado mediante Talk 6.
Set	Establece de manera dinámica el temporizador de antigüedad Path MTU (PMTU).
Stats	Visualiza estadísticas de todos los túneles o de un túnel activo.
Exit	Hace volver al nivel de mandato anterior. Consulte “Salida de un entorno de nivel inferior” en la página xxv.

Change Tunnel

Cambia de manera dinámica un túnel seguro.

Sintaxis:

change tunnel ...

Consulte la descripción del mandato **add tunnel** en “Mandatos de configuración de seguridad IP manual” en la página 359 si desea obtener una descripción de los parámetros.

Delete Tunnel

Utilice el mandato **delete** para suprimir de manera dinámica un túnel seguro o todos los túneles seguros.

Sintaxis:

delete t**unnel**

id-túnel
nombre-túnel
all

id de túnel
Especifica el identificador del túnel IPSec que se debe suprimir.

Valores válidos: 1 - 65535

Valor por omisión: 1

nombre de túnel
Especifica el nombre del túnel IPSec que se debe suprimir.

Valores válidos: cualquier nombre de túnel configurado

Valor por omisión: ninguno

all Especifica que todos los túneles IPSec de esta interfaz deben ser suprimidos.

Disable

Utilice el mandato **disable** para inhabilitar de manera dinámica el protocolo de seguridad IP en todas las interfaces o en un solo túnel.

Sintaxis:

di**sable**
ipsec drop
ipsec pass
tunnel ...

ipsec drop
Inhabilita la seguridad IP en el direccionador de manera segura. Todos los túneles IPSec se inhabilitarán pero la información de túnel seguro de las normas de filtro de paquetes se utiliza para identificar los paquetes que coinciden con los filtros de paquetes de túnel IPSec. Los paquetes coincidentes se eliminan.

ipsec pass
Inhabilita la seguridad IP en el direccionador de manera no segura. Se inhabilitarán todos los túneles IPSec. Los paquetes que coinciden con los filtros de paquetes de túnel se reenvían como tráfico ordinario.

tunnel *id-túnel* **all**
Inhabilita la seguridad IP en un túnel especificado o en todos los túneles.

id de túnel
Especifica el identificador del túnel seguro que se debe inhabilitar.

Valores válidos: 1 - 65535

Valor por omisión: 1

all Todos los túneles.

Enable

Utilice el mandato **enable** para habilitar de manera dinámica el protocolo de seguridad IP en todas las interfaces o en un solo túnel. Debe habilitar IPSec de manera global en el direccionador antes de que los túneles IPSec habilitados de manera individual se activen.

Nota: No se puede habilitar dinámicamente a IPSec si el direccionador se ha reiniciado con IPSec inhabilitado.

Sintaxis:

enable
ipsec
tunnel ...

ipsec
Habilita la seguridad IP a través del direccionador.

tunnel *id-túnel* **| all**

id de túnel
Especifica el identificador del túnel seguro que se debe habilitar.

Valores válidos: 1 - 65535

Valor por omisión: 1

all Todos los túneles.

List

Utilice el mandato **list** para visualizar la configuración de seguridad IP actual. Los túneles globales incluyen todos los túneles del direccionador, tanto activos como definidos. Todos los túneles incluyen todos los túneles configurados en esta interfaz, tanto activos como definidos. Los túneles activos son los que están activos en este momento; los túneles definidos son los que están definidos pero no están activos.

Sintaxis:

list ...
all
global
tunnel
active *id-túnel nombre-túnel* all
defined *id-túnel nombre-túnel* all

Ejemplo 1: Listado 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: Listado de un túnel activo que haya recibido un mensaje de “paquete demasiado grande”

```
IPV6-IPsec>li tun act 1

Tunnel      Name       Mode  Policy  Life  Replay       Tunnel       PMTU
  ID                                      Prev      Expiration
------ --------------- ----- ------ ------ ------ ------------------ -----
     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 PMTU aparece como n/a si no se ha recibido ningún paquete demasiado grande.

2 Es una dirección IPv6. Si la versión IP es IPv4, se visualiza un mensaje que define el manejo del bit DF: COPY, SET o CLEAR.

Ejemplo 3: Listado 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 de manera dinámica la seguridad IP en el direccionador o en un solo túnel. Después de reiniciar IPSec o los túneles, asegúrese de que utiliza el mandato **reset IP** para restablecer la configuración IP. Esto es necesario para volver a cargar información del control de acceso como los filtros de paquetes y sus normas de control de acceso. Si no restablece IP, es probable que los filtros de paquetes y las normas de control de acceso no ofrezcan soporte a la nueva configuración IPSec.

Como alternativa a la utilización de los mandatos **reset**, se puede rearrancar el direccionador. De todos modos, si rearranca el direccionador, lo aísla de la red durante unos instantes, mientras que los mandatos **reset** sólo interrumpen las funciones de IP.

Sintaxis:

r**eset**

ipsec
tunnel *id-túnel nombre-túnel* all

ipsec

Restablece la seguridad IP en el 2212. La seguridad IP se inhabilita de manera temporal y, a continuación, se reinicia. Mientras la seguridad IP está inhabilitada, los paquetes que normalmente manejan los túneles IPSec se eliminan hasta que el reinicio ha finalizado. Reiniciar la seguridad IP no afecta a otras funciones del 2212. Este mandato activa la configuración de seguridad que se ha creado mediante Talk 6. La configuración de seguridad IP de Talk 6 sobreescribe la configuración Talk 5.

tunnel

Restablece la seguridad IP en un túnel especificado. Si el túnel está inhabilitado en el momento del reinicio, la configuración del túnel se

reconstruye a partir de la configuración de SRAM, pero el túnel permanece inhabilitado después del reinicio.

id de túnel
Especifica el identificador del túnel seguro a iniciar.

Valores válidos: 1 - 65535

Valor por omisión: 1

nombre de túnel
Especifica el nombre del túnel seguro a iniciar.

Valores válidos: cualquier nombre de túnel configurado

Valor por omisión: ninguno

all Todos los túneles.

Set

Establece de manera dinámica el temporizador de antigüedad Path MTU (PMTU).

Sintaxis:

set path

path
Este parámetro define el tiempo en minutos que transcurrirá antes de que el 2212 establezca de nuevo MTU en su valor máximo.

Valor por omisión: 10 (0 significa inhabilitado)

Stats

Utilice el mandato **stats** para visualizar estadísticas sobre un túnel específico o sobre todos los túneles. Por ejemplo, el mandato **stats** muestra los paquetes enviados y recibidos.

Sintaxis:

stats
id-túnel
nombre-túnel
all

id de túnel
Especifica el identificador del túnel seguro.

Valores válidos: 1 - 65535

Valor por omisión: 1

nombre de 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 sobre todos los túneles configurados en el 2212.

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 IP manual (IPv6)

Esta sección explica la manera de supervisar IPSec manual con IPv6. Describe la manera de acceder al entorno de seguridad IP y los mandatos disponibles.

Acceso al entorno de supervisión de la seguridad IP

Para acceder al entorno de supervisión de la seguridad 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 IP (IPv6)

Los mandatos de supervisión de la seguridad 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 IP (IPv4)” en la página 381 si desea obtener una descripción de los mandatos. Entre los mandatos en el indicador IPV6-IPsec>.

Mandatos de supervisión de la seguridad IP (talk 5)

Capítulo 22. Utilización de la función de servicios diferenciados

En este capítulo se describe la manera de utilizar la función de servicios diferenciados (DiffServ) para que un direccionador pueda proporcionar servicio preferente a los paquetes de datos IP adecuados. Según la información de la cabecera IP, el direccionador clasifica paquetes comparándolos con las configuraciones predefinidas en la base de datos de política (creada con la función de política). Consulte el Capítulo 18, “Utilización de la función de política” en la página 275 si desea obtener información detallada al respecto. Como resultado, algunos paquetes pueden recibir servicio preferente. Este capítulo consta de las siguientes secciones:

- “Visión general de los servicios diferenciados”
- “Terminología de los servicios diferenciados” en la página 392
- “Configuración de los servicios diferenciados” en la página 392

Visión general de los servicios diferenciados

La mayoría de dispositivos de reenvío instalados en una red IP ofrecen el servicio estándar optimizado para los paquetes de datos según el modelo "primero en llegar, primero en ser servido". Este método de entrega es el adecuado para la mayoría de tráfico pero emergen nuevas aplicaciones que requieren una transmisión más rápida y fácil de algunos paquetes.

La función de servicios diferenciados (DiffServ) proporciona diferentes niveles de servicio a paquetes IP cuando un direccionador los procesa para transmisión. DiffServ proporciona a algunos paquetes servicio preferente al reservarles recursos del sistema (almacenamientos intermedios) y recursos de enlace (ancho de banda). Una función clasificadora DiffServ determina el tipo de servicio que se ofrece a los paquetes IP examinando varios campos en la cabecera IP, por ejemplo, rangos de direcciones de origen y destino y números de puerto, el tipo de protocolo y el byte TOS entrante. Para llevarlo a cabo de una manera adaptable, los flujos individuales se agregan para formar las corrientes. Las corrientes son las entidades mediante las que DiffServ gestiona el acceso a almacenamientos intermedios y ancho de banda. La Figura 38 muestra cómo DiffServ procesa los paquetes de una corriente.

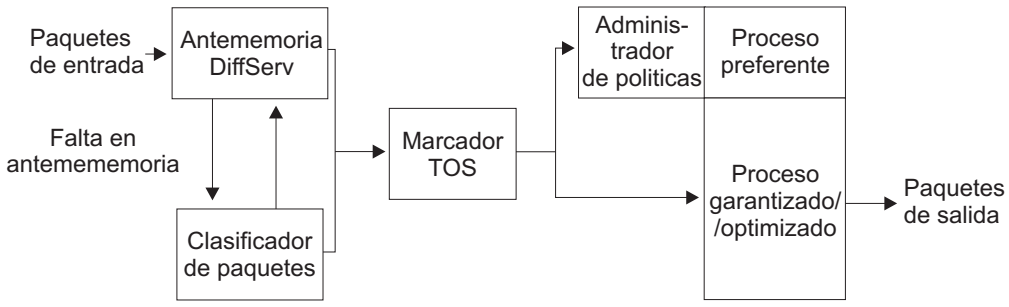


Figura 38. Vía de acceso de paquetes de datos de DiffServ

Además del servicio tradicional optimizado, DiffServ proporciona los siguientes tipos de servicio:

Utilización de los servicios diferenciados

Reenvío acelerado (EF)

El servicio de reenvío acelerado representa la implementación por parte de DiffServ de un servicio preferente y ambos términos se utilizan indistintamente en el texto siguiente. Este servicio garantiza una velocidad de transmisión específica y un retraso menor que el servicio de reenvío garantizado u optimizado. Si se genera demasiado tráfico, DiffServ elimina el tráfico sobrante. La cola preferente proporciona servicio EF y aparece en la Figura 39 en la página 391 como cola EF.

Reenvío garantizado (AF)

El servicio de reenvío garantizado representa la implementación por parte de DIffServ de un servicio garantizado y ambos términos se utilizan indistintamente en el siguiente texto. Este servicio garantiza una velocidad de transmisión específica, pero no dispone de garantía en cuanto a retrasos. Si existen recursos desocupados, DiffServ puede enviar el tráfico sobrante a una velocidad mayor. La cola AF/BE proporciona servicio AF y aparece en Figura 39 en la página 391.

Optimizado (BE)

Se trata del servicio optimizado estándar que no proporciona garantías en cuanto a servicio ni en cuanto a retrasos. Se debe encontrar un equilibrio entre reservar recursos para los servicios EF y AF y dejar suficientes recursos libres para que el tráfico optimizado reciba un servicio adecuado. La cola AF/BE proporciona servicio BE y aparece en Figura 39 en la página 391.

Los direccionadores locales crean y envían paquetes de control, por lo que que también debe dejar suficientes recursos libres para que reciban un servicio adecuado.

Actualmente DiffServ se implementa en enlaces PPP y Frame Relay y puede ser utilizado por el subsistema RSVP. La Figura 38 en la página 389 muestra cómo se procesan los paquetes de una corriente. Cuando un direccionador recibe el primer paquete de un flujo (presuponiendo siempre que se haya designado para un servicio preferente), no existe ninguna indicación de su categoría de servicio en la antememoria de vía rápida, de manera que el paquete es procesado por la vía lenta. DiffServ invoca una búsqueda de la base de datos de políticas para obtener los criterios de manejo de paquetes (política). La acción definida por la política se guarda en la antememoria de vía rápida. Cuando el direccionador recibe un paquete posterior de este flujo, ya existe una entrada en la antememoria de vía rápida para dicho flujo con lo que se aplica la acción definida por la política y el paquete toma la vía rápida. Por lo tanto, los paquetes posteriores procedentes de este flujo reciben un servicio preferente.

La Figura 39 en la página 391 muestra la relación entre el administrador de políticas, la gestión del almacenamiento intermedio, las colas y el planificador—algunos de los componentes básicos que proporcionan diferente calidad de niveles de servicio.

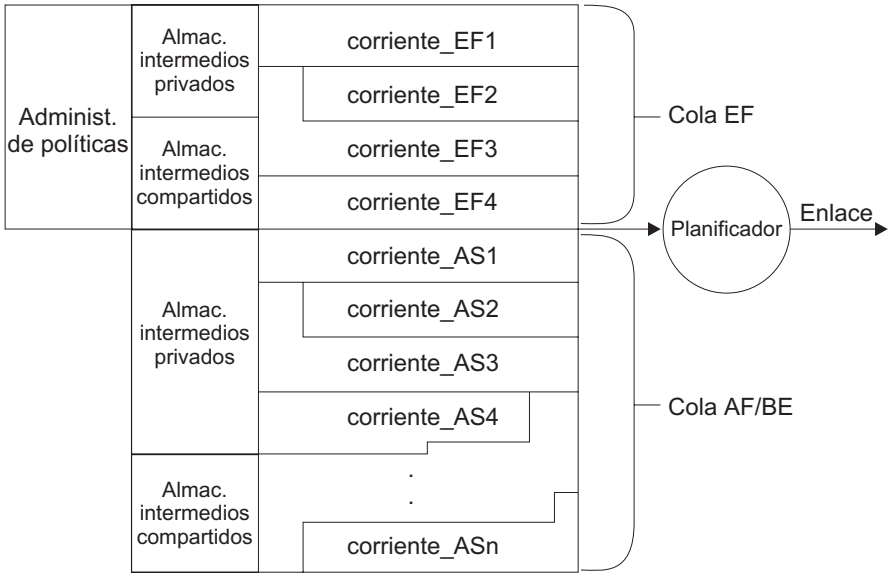


Figura 39. Relación entre almacenamientos intermedios, colas y planificador

Los servicios de reenvío acelerado (EF) y reenvío garantizado (AF) disponen de diferentes características que reciben el soporte de tres funciones del direccionador: (1) El administrador de políticas, (2) la gestión de almacenamiento intermedio y (3) el planificador. Dichas funciones proporcionan un control de tráfico más sofisticado que el disponible en un dispositivo direccionador BE tradicional.

Si el tráfico requiere proceso de EF, el tráfico sobrante debe ser eliminado. La función de *administrador de políticas* de DiffServ utiliza un método (token bucket) para examinar el tráfico de EF y determinar si sobra un paquete. Si es así, el administrador de políticas elimina el paquete.

Si el tráfico es para AF, BE, o se trata de tráfico de EF que el administrador de políticas ha permitido, la función de *gestión del almacenamiento intermedio* basada en la velocidad lo procesa. Esta función asigna almacenamientos intermedios para la interfaz desde una agrupación privada o desde una agrupación compartida común para todas las interfaces. Utilice el mandato de configuración **set receive-buffers** de Talk 6 (consulte el mandato set receive-buffers de la publicación *Software de Access Integration Services Guía del usuario*) para especificar la cantidad total de espacio de almacenamiento intermedio físico disponible para una interfaz. Utilice el mandato **set interface** de Talk 6 para establecer el tamaño del almacenamiento intermedio de salida de las colas de servicio preferente y garantizado. Es el espacio de almacenamiento intermedio que DiffServ gestiona. (DiffServ gestiona dos agrupaciones independientes—una para la cola preferente (EF) y la otra para la cola de reenvío garantizado (AF). (Asegúrese de que el espacio de almacenamiento intermedio que especifique refleje la cantidad real de espacio de almacenamiento intermedio disponible en el sistema). La gestión de almacenamiento intermedio determina si los almacenamientos intermedios de la agrupación privada de su interfaz están disponibles para el paquete. Si lo están, acepta el paquete y lo pone en cola. Si no lo están, intenta asignar espacio de almacenamiento intermedio de la agrupación compartida y, si lo consigue, pone en cola el paquete. Si no hay espacio de almacenamiento intermedio compartido, la gestión del almacenamiento intermedio elimina el paquete.

La función *planificador* examina las colas regularmente, retira de la cola los paquetes que están en cola y los envía al adaptador de la interfaz para su transmisión. Se trata de un planificador de colocación en cola equilibrada

autosincronizado, lo cual es una variación de la colocación en cola equilibrada ponderada. Puede configurar los factores de ponderación del planificador y especificar la frecuencia con la que el planificador examina las colas.

Nota: Se pueden configurar opciones de DiffServ de tal manera que los recursos se comprometan o se reserven en exceso, es decir, los controles del condicionador de tráfico están configurados como si hubiera más ancho de banda o almacenamiento intermedio que los que hay realmente disponibles. DiffServ no ofrece soporte a los excesos de reservas.

Si una corriente DiffServ queda desocupada (no se han enviado paquetes en la corriente durante algún tiempo), el sistema reclama los recursos para que otras corrientes puedan utilizarlos. Si el sistema se reactiva, los recursos vuelven a él. Si los recursos ya no están disponibles a causa de un exceso de reserva, DiffServ intenta de manera periódica volver a asignar los recursos.

Después de haber utilizado la función de política para configurar las políticas adecuadas, el primer paso para implementar DiffServ es utilizar el mandato **set** de DiffServ para configurar las opciones que definen los recursos del sistema disponibles para DiffServ. A continuación, utilice el mandato **enable ds** para habilitar la función DiffServ y el mandato **enable interface** para habilitar la interfaz de salida.

Terminología de los servicios diferenciados

Los siguientes términos se utilizan para describir DiffServ:

Antememoria de DiffServ
Esta antememoria contiene el tráfico y el perfil de servicio de los flujos IP activos más recientes servidos por el direccionador.

Flujo
Secuencia de paquetes con el mism puerto y dirección de origen, protocolo IP y puerto y dirección de destino.

Corriente
Agregación de flujos.

Interfaz virtual (VIF)
En el caso de los enlaces Frame Relay, cada conexión DLCI se considera una interfaz virtual.

Configuración de los servicios diferenciados

El siguiente procedimiento proporciona una descripción paso a paso sobre el modo de configurar DiffServ a fin de proporcionar un servicio preferente a los paquetes seleccionados. En primer lugar, debe acceder a la función DiffServ:

1. En el indicador `*`, entre **talk 6**.
2. En el indicador `Config>`, entre **feature ds**. A continuación aparece el indicador `DS config>` y se abre el diálogo de configuración.

```
* talk 6
Config>feature ds
DS config>
```

3. Habilite la función DiffServ en un direccionador:

```
DS config>enable ds
DiffServ enabled
```

4. Habilite y establezca los parámetros de la 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 de Cola preferente y Cola garantizada/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, el 20 por ciento del ancho de banda de línea y el 90 por ciento de la carga del planificador se conceden a la cola EF. El tamaño del almacenamiento intermedio de salida de la cola EF es 5500 (en bytes), del que un 95 por ciento se puede asignar a corrientes QOS. El tamaño del almacenamiento intermedio de salida de la cola AF/BE es 27500 (en bytes), del que un 80 por ciento se puede asignar a corrientes QOS.

5. Cuando haya acabado de habilitar DiffServ en los direccionadores y de establecer los parámetros, entre **Ctrl-P** para volver al indicador *.

Después de habilitar DiffServ y establecer los parámetros de interfaz, debe reiniciar o volver a cargar el dispositivo para activar DiffServ. Si desea obtener información más detallada sobre cómo especificar los mandatos de DiffServ, consulte el Capítulo 23, “Configuración y supervisión de la función de servicios diferenciados” en la página 395.

Capítulo 23. Configuración y supervisión de la función de servicios diferenciados

Esta capítulo describe los mandatos que la función de servicios diferenciados (DiffServ) proporciona para la configuración de direccionadores e interfaces a fin de facilitar un servicio preferente para paquetes de datos seleccionados. Consta de 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 400
- "Mandatos de supervisión de los servicios diferenciados" en la página 401

Acceso al indicador de configuración de los servicios diferenciados

Para entrar los mandatos de configuración de DiffServ:

1. Entre **talk 6** en el indicador OPCON (*).
2. Entre **feature ds** en el indicador Config>.

Aparece el indicador DS Config>. Ahora ya puede entrar los mandatos de configuración de DiffServ.

Mandatos de configuración de los servicios diferenciados

Estos mandatos le permiten configurar las opciones de DiffServ, las cuales determinan un servicio preferente para los paquetes de datos seleccionados. La Tabla 47 resume los mandatos de configuración y el resto de esta sección los describe de manera detallada. Entre los mandatos en el indicador DS Config>. Entre el mandato y las opciones en una línea o entre sólo el mandato y, a continuación, responda a las solicitudes. Para ver una lista de las opciones de mandato, entre el mandato con un interrogante en lugar de las opciones.

Tabla 47. Mandatos de configuración de DiffServ

Mandato	Función
? (Ayuda)	Visualiza todos los mandatos disponibles para este nivel de mandato, o lista las opciones de mandatos específicos (si es que están disponibles). Consulte "Obtención de ayuda" en la página xxv.
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 información sobre el sistema DiffServ de un direccionador y los valores relacionados con la interfaz.
Set	Especifica los valores de un direccionador relacionados con DiffServ.
Exit	Hace volver al nivel de mandato anterior. Consulte "Salida de un entorno de nivel inferior" en la página xxv.

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 del direccionador.

Ejemplo:

```
DS Config> delete ds
Diffserv system config record deleted
```

interface
Le solicita el número de interfaz 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 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 a habilitar.

Ejemplo:

```
DS Config> enable interface
Enter Interface number [0]? 2
DiffServe interface enabled
```

Nota: DiffServ sólo se puede habilitar en enlaces PPP y Frame Relay.

List

Utilice el mandato **list** para visualizar información sobre el sistema DiffServ y los valores relacionados con la interfaz de un direccionador.

Sintaxis: list all
ds
interface

all Visualiza información sobre las configuraciones de DiffServ y de interfaz de un direccionador.

ds Visualiza la configuración 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 de un direccionador, su estado de habilitación/inhabilitación de DiffServ y los parámetros de cada interfaz y de cada cola.

Ejemplo:

```
DS Config> list interface
-------------------------------------------------------------------------------
                          ---------- Premium -------   --------- Assured --------
Net If     Status  NumQ Bwdth  Wght  OutBuf  MaxQos Bwdth  Wght  OutBuf  MaxQos
Num                       (%)   (%) (bytes)     (%)   (%)   (%) (bytes)     (%)
-------------------------------------------------------------------------------
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 establecer el sistema DiffServ de un direccionador y los parámetros relacionados con la interfaz.

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 a asignar al servicio optimizado.

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 a asignar al servicio de control de la 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 que se debe habilitar para DiffServ y le solicita los parámetros específicos de la interfaz.

Ancho de banda de la cola

Especifica el porcentaje del enlace de salida que se debe utilizar para la cola preferente. El porcentaje restante se utiliza para el valor de cola garantizada.

Valor por omisión: 20

Peso de cola

Especifica el porcentaje de tiempo durante el cual el planificador supervisa la cola preferente. El porcentaje restante se utiliza para el valor de cola garantizada. El valor por omisión del peso de cola es 90 por ciento a fin de que el planificador reaccione con rapidez ante el tráfico EF.

Valor por omisión: 90

Tamaño de almacenamiento intermedio de salida

Especifica la cantidad de datos (en bytes) que se pueden poner en la cola preferente y en la cola garantizada.

En el caso de la cola preferente, este parámetro controla la cantidad de datos (en bytes) que se pueden colocar en la cola preferente. Si se establece un valor demasiado alto para este parámetro, se puede generar un gran retraso en la colocación en cola del tráfico preferente. Por ejemplo, si se establece en 25 Kbytes y la velocidad de enlace de

salida es 1,5 Mbps (velocidad T1), en ese caso existe un posible retraso de colocación en cola de 133 mseg (25000 bytes * 8 bits/byte)/1500000 bps o 0,133 seg (133 milisegundos). Si se establece un valor demasiado bajo para este parámetro, será imposible colocar ráfagas pequeñas en almacenamiento intermedio. Por ejemplo, si se establece en 2 Kb, ello implica que no habrá suficiente almacenamiento intermedio para una ráfaga de 2 paquetes de 1500 bytes (ya que requieren 3000 bytes de espacio de almacenamiento intermedio).

Como equilibrio entre estos dos extremos, el valor por omisión es 5500 bytes, que es diez veces el tamaño del paquete por omisión (550).

Valor por omisión: 5500 (cola preferente)

En el caso de la cola garantizada, este parámetro controla la cantidad de datos (en bytes) que se pueden colocar en la cola garantizada. Las consideraciones sobre este valor de parámetro son las mismas que para la cola preferente, excepto por el hecho de que el tráfico de la cola garantizada no dispone de requisitos de retraso muy estrictos. Más bien, es más probable que el tráfico de cola garantizada consista en flujos TCP, que son ráfagas por naturaleza. Es por ello que se debe definir el suficiente espacio de almacenamiento intermedio a fin de dar cabida a ráfagas procedentes de varios flujos.

El valor por omisión es 27500, que es cincuenta veces el tamaño del paquete por omisión (550).

Valor por omisión: 27500 (cola garantizada)

Asignación de QoS de salida

Especifica la cantidad de tamaño del almacenamiento intermedio de salida (expresada en porcentaje) que todas las corrientes DiffServ pueden reservar. El porcentaje restante se utiliza para el tamaño mínimo de la agrupación compartida.

Valor por omisión: 95 (cola preferente)

Valor por omisión: 80 (cola garantizada)

Ejemplo:

Supervisión de DiffServ (talk 5)

```
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). Ello permite que DiffServ determine el espacio de almacenamiento intermedio disponible en las interfaces de entrada y de salida. Si este valor se modifica, se debe reiniciar el direccionador y los valores del mandato **set interface** deben ser revisados y cambiados, si fuera 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 la consola de la función DiffServ le permite ver y gestionar los valores relacionados con DiffServ. Para acceder al entorno de supervisión, entre **talk 5** en el indicador OPCON (*):

```
* t 5
```

A continuación, entre el mandato siguiente en el indicador **+**:

```
+ feature ds
DS Console>
```

Mandatos de supervisión de los servicios diferenciados

Estos mandatos le permiten ver los valores relacionados con DiffServ. La Tabla 48 resume los mandatos de supervisión de DiffServ y el resto de la sección los describe. Entre los mandatos en el indicador `DS Console>`. Entre el mandato y las opciones en una línea o entre sólo el mandato y, a continuación, responda a las solicitudes. Para ver una lista de las opciones de mandato, entre el mandato con un interrogante en lugar de las opciones.

Tabla 48. Mandatos de supervisión de DiffServ

Mandato	Función
? (Ayuda)	Visualiza todos los mandatos disponibles para este nivel de mandato, o lista las opciones de mandatos específicos (si es que están disponibles). Consulte “Obtención de ayuda” en la página xxv.
Clear	Borra estadísticas de una corriente entre un par de interfaces de entrada y de salida específicas.
DScache	Borra o visualiza información sobre la antememoria de DiffServ de un direccionador.
List	Visualiza información sobre el sistema DiffServ de un direccionador y los valores relacionados con la interfaz.
Exit	Hace volver al nivel de mandato anterior. Consulte “Salida de un entorno de nivel inferior” en la página xxv.

Clear

Utilice el mandato **clear** para borrar las estadísticas de una corriente entre un par de interfaces de entrada y salida específicas.

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 de la antememoria de DiffServ de un direccionador.

Sintaxis: dscache actions
clear
nexthop
order
stats

actions

Visualiza las acciones que se deben llevar a cabo para los paquetes enviados desde el origen IP especificado al destino IP especificado, y el ID de corriente de DiffServ, si lo hay.

Ejemplo:

Mandatos de supervisión de DiffServ (talk 5)

```
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 del salto siguiente.

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 el 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 al destino IP especificados.

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 sobre el sistema DiffServ y los valores relacionados con la interfaz de un direccionador.

Sintaxis: list interface
queue
stream
vifs

interface

Lista las interfaces de un direccionador, su estado de habilitación/inhabilitación de DiffServ y sus asignaciones de almacenamiento intermedio, además de otra información.

Net Visualiza el número de la 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, si el enlace no es DiffServ, o bien 0, si no hay paquetes en proceso).

InMax Visualiza el tamaño de almacenamiento intermedio máximo configurado para el reenvío garantizado.

InCurr
Visualiza la cantidad de espacio de almacenamiento intermedio que se está utilizando en este momento para la corriente de entrada. Los almacenamientos intermedios contienen paquetes en proceso.

InShar
Visualiza la cantidad de espacio de almacenamiento intermedio compartido disponible para esta interfaz de salida.

InMaxA
Visualiza la cantidad máxima de espacio de almacenamiento intermedio que se puede asignar a todas las corrientes QoS en agregado.

InCurA
Visualiza la cantidad de espacio de almacenamiento intermedio asignado disponible que la corriente de entrada puede utilizar.

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 colocados en cola actualmente (0 indica que no hay paquetes en cola en este momento).

Svc Tag
Visualiza la siguiente hora virtual en que esta cola debe recibir servicio.

Weight
Visualiza el peso del planificador de esta cola.

out_max_alloc
Visualiza la cantidad máxima de espacio de almacenamiento intermedio que se puede asignar a una corriente de 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 de esta cola.

out_curr_buff
Visualiza la cantidad de espacio de almacenamiento intermedio asignado actualmente que se está utilizado para paquetes.

out_share_buff
Visualiza la cantidad de espacio de almacenamiento intermedio que se halla en este momento 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 sobre corrientes.

Id Número de identificación de la corriente

t Tipo de corriente

- **D** Corriente de DiffServ
- **B** Corriente optimizada
- **C** Corriente de control de red
- **R** Corriente RSVP

I/o q Tipo de cola

q1 Cola preferente

q2 Cola garantizada/BE

allo/cur(K)
Espacio total de almacenamiento intermedio (en kilobytes) asignado por esta corriente.

tot pkt
Número total de paquetes recibidos por esta corriente para su transmisión.

tot Kby
Cantidad total de kilobytes recibidos por esta corriente para su transmisión.

pkt snt
Número total de paquetes enviados por esta corriente.

Kby snt
Número total de kilobytes enviados por esta corriente.

ovr snt
Número de paquetes enviados mediante 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 administrador de políticas en la cola preferente.

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 sobre las interfaces virtuales Frame Relay.

Ejemplo:

Mandatos de supervisión de DiffServ (talk 5)

```
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
```

Capítulo 24. Utilización de túneles de capa 2 (L2TP, PPTP, L2F)

Los túneles de capa 2 (L2T) constan de los protocolos de túnel L2TP, L2F y PPTP.

El protocolo de túnel de capa 2 (L2TP) es un protocolo de pistas de estándares IETF para túneles PPP en una red de paquetes, tal como UDP/IP. L2TP está orientado a la conexión.

El reenvío de capa 2 (L2F) y el protocolo de túnel punto a punto (PPTP) son protocolos informativos IETF para túneles PPP en una red IP.

Visión general de L2TP

L2TP permite que muchos dominios de protocolo independientes y autónomos compartan una infraestructura de acceso común que incluye módems, Access Servers y direccionadores RDSI. L2TP permite los túneles de la capa de enlace PPP, por ejemplo, HDLC y HDLC asíncrono. Mediante dichos túneles, es posible disociar la ubicación del servidor de marcación contactado de la ubicación que proporciona acceso a la red.

Tradicionalmente, el servicio de red de marcación de Internet se proporciona sólo para 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 ofrecer soporte a conexiones de marcación IP, IPX y AppleTalk direccionadas a través de PPP en una infraestructura de Internet existente de forma privada.

El soporte de estas aplicaciones de marcación virtual de varios protocolos es beneficioso para usuarios finales, empresas y proveedores de servicios de Internet porque permite compartir inversiones significativas en infraestructuras de acceso y básicas y permite que los usuarios efectúen llamadas locales para acceder a los servicios.

L2TP permite también el uso seguro de las inversiones existentes en aplicaciones de protocolo no IP dentro de la infraestructura de Internet existente.

La Figura 40 muestra un ejemplo de red L2TP que utiliza RDSI. La red puede utilizar cualquier tipo de medio entre el L2TP Network Access Concentrator (LAC) y el L2TP Network Server (LNS).

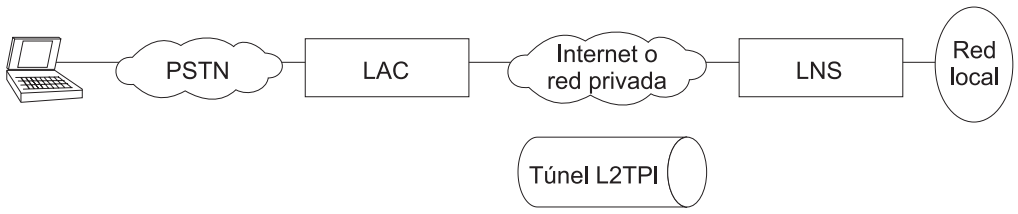


Figura 40. Ejemplo de red L2TP

Términos de L2TP

Los siguientes términos se utilizan para describir L2TP:

Attribute Value Pair (AVP)
Método uniforme de codificar tipos y cuerpos de mensajes. Este método maximiza la capacidad de extensión a la vez que permite la interoperatividad de L2TP.

L2TP Access Concentrator (LAC)
Dispositivo conectado a una o más redes telefónicas de servicio público (PSTN) o líneas RDSI capaces de manejar tanto el funcionamiento de PPP como el protocolo L2TP. El LAC implementa el medio sobre el que trabaja L2TP. L2TP pasa el tráfico a uno o más L2TP Network Servers (LNS). L2TP puede crear un túnel para cualquier protocolo transportado por la red PPP.

L2TP Network Server (LNS)
Un LNS trabaja en cualquier plataforma que pueda ser una estación final PPP. El LNS maneja el lado servidor del protocolo L2TP. Como L2TP sólo confía en el único medio por el que llegan los túneles L2TP, el LNS sólo puede disponer de una interfaz LAN o WAN, aunque aún pueda interrumpir llamadas procedentes de cualquier interfaz PPP que reciba soporte de un LAC.

Network Access Server (NAS)
Dispositivo que proporciona a los usuarios acceso temporal a la red, a petición. Dicho acceso se efectúa punto a punto mediante líneas PSTN o RDSI.

Sesión (llamada)
L2TP crea una sesión cuando se intenta una conexión PPP de extremo a extremo entre un usuario de marcación y el LNS. Los datagramas de la sesión se envían sobre el 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 viene definido por un par de LNS-LAC. El túnel transporta los datagramas PPP entre el LAC y el LNS. Un único túnel puede multiplexar muchas sesiones. Una conexión de control que opera sobre el mismo túnel controla el establecimiento, la liberación y el mantenimiento de todas las sesiones y del propio túnel.

Funciones que reciben soporte

L2TP se ejecuta en UDP/IP y ofrece soporte a las siguientes funciones:

- Túneles de clientes de marcación de un único usuario.
- Túneles de direccionadores pequeños, por ejemplo un direccionador con una única ruta estática a definir según un perfil de usuario autenticado.
- Las llamadas se pueden iniciar desde el LAC al LNS (entrada), desde el LNS al LAC (salida) o por cualquiera de los dos nodos. Las llamadas de salida pueden ser una sesión de túnel L2 *fija* (siempre activa) o una sesión de túnel L2 basada en la demanda.
- Varias llamadas por túnel.
- Autenticación proxy para PAP, CHAP y MS-CHAP.
- Proxy LCP.
- Reinicio de LCP en el caso de que Proxy LCP no se utilice en el LAC.
- Autenticación de punto final de túnel.
- AVP oculto para transmisión de una contraseña PAP de proxy.

- Túneles mediante una tabla de búsqueda de reinos (es decir usuario@reino).
- Túneles mediante la búsqueda de nombres de usuario PPP en el subsistema AAA.
- Gestión de túneles L2TP mediante SNMP. Consulte “Gestión SNMP” en la publicación *Configuración y supervisión de protocolos - Manual de consulta Volumen 1*.

Nota: Los túneles de reino requieren nombres de usuario en el formato *nombre@reino*. Este tipo de túneles requieren software para consultar dos tablas a fin de resolver el destino al que el usuario de marcación accede mediante un túnel. La ventaja de utilizar este método de creación de túneles es que sólo es necesario definir el reino y los nombres de usuario que coincidan con el reino accederán al mismo destino mediante el túnel.

La creación de túneles basada en usuarios se resuelve en una única tabla. Le permite la granularidad de dirigir cada usuario a un destino exclusivo mediante túneles.

- BRS para un LNS (como punto final PPP).
- Capacidad de utilizar el mandato **delete interface** para suprimir dispositivos L2TP.
- Capacidad de volver a configurar de manera dinámica dispositivos L2TP.
- Establecimiento de un canal de control de secuencia, colas, retransmisión y flujo. L2TP también lleva a cabo el control de secuencia, cola y flujo en canales de datos.
- Capacidad de corregir el puerto L2TP UDP (1701) para que se puedan establecer filtros de Seguridad IP basados en el puerto UDP.
- Un cliente de direccionador L2TP. Un cliente de direccionador L2TP es un modelo “iniciado por cliente” (también conocido como creación de túneles voluntaria). Esta función proporciona servicios Virtual Private Network (VPN) multiprotocolo, por túnel y seguros, independientemente de la topología del proveedor de servicios. Esta función junta al cliente y al LAC en una unidad física de hardware.
- Conexión de una llamada de entrada a la interfaz adecuada según una coincidencia de nombre de sistema principal remoto. Si el nombre del sistema principal remoto no coincide con ninguna de las interfaces configuradas para la coincidencia de nombres de sistema principal, la llamada se realiza en una interfaz de entrada que no utiliza la coincidencia de nombres de sistema principal remoto.

  Nota: Si ha configurado varias correlaciones de red entre el mismo par de LAC - LNS, asegúrese de que sólo existe un túnel para cada correlación.

- Configuración automática de IP, IPX y de puentes de redes de entrada que no utilizan la coincidencia de nombres de sistema principal remoto. Debe configurar manualmente las redes de salida y las redes de entrada que utilizan la coincidencia de nombres de sistema principal remoto.

Otros protocolos de túnel de capa 2 con soporte son:

- Tanto las funciones NAS como de pasarela de L2F reciben soporte.
- El cliente de direccionador de PPTP, el PAC (concentrador de acceso de PPTP) y el PNS (servidor de red de PPTP) reciben soporte.

Utilización de túneles de capa 2

L2F proporciona túneles de capa 2 con capacidad de interoperación al conectar con dispositivos de red que no ofrecen soporte a L2TP.

PPTP proporciona túneles de capa 2 con capacidad de interoperación al conectar con dispositivos de red que no ofrecen soporte a L2TP. PPTP se puede utilizar de manera específica para servicios VPN desde Microsoft Windows 95 (DUN 1.2 y posteriores), Windows 98 y Windows NT a direccionadores IBM.

Nota: Tanto L2F como PPTP se configuran en la función de túnel de capa 2.

Consideraciones de tiempo

La creación de túneles para paquetes PPP en redes direccionadas genera algunas circunstancias relacionadas con el tiempo que se deben tener en cuenta. L2TP presupone que la conexión entre el LAC y LNS no sufre un retraso lo suficientemente largo para exceder el tiempo de espera de los iguales conectados mediante túnel. Si la latencia entre iguales alcanza o supera repetidamente la del tiempo de espera de la máquina de estado PPP (normalmente 3 segundos), la conectividad puede verse entorpecida. Observe que si la latencia entre el LAC y LNS es tan pobre, la conectividad en general es tan pobre que la conexión no será razonable aunque las máquinas de estado PPP se mantengan vivas artificialmente. Si ambas partes poseen dicha capacidad, se puede ampliar el tiempo de espera PPP para alcanzar la conectividad en una conexión muy pobre.

Además de la latencia, una discrepancia de ancho de banda entre el par LAC/LNS y el par LAC/cliente puede ocasionar problemas. Por ejemplo, si 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 dedicar un tiempo considerable a intentar enviar paquetes al LNS. Por otra parte, si la conexión entre el LNS y un sistema principal en una red local LNS es excepcionalmente rápida comparada con el cliente de marcación, es probable que se sobrecargue el LNS al intentar enviar datos al LAC. L2TP implementa una serie de técnicas de control de flujo interno y externo en un intento de combatir estas situaciones.

Consideraciones sobre LCP

Al utilizar Proxy LCP, el LAC negocia el LCP y PPP continúa procesando en el LNS. El LAC envía opciones LCP al LNS para que el LNS esté al corriente de lo que se ha negociado. El LNS debe continuar siendo flexible a los parámetros negociados por el cliente y el LAC. Si existen parámetros que no son aceptables para el LNS, L2TP intenta volver a negociar el LCP enviando una *Petición de configuración de LCP* al cliente a través del túnel.

El requisito de que el LNS continúe siendo flexible es de especial importancia por lo que se refiere al MRU. En el IBM LNS, el MRU configurado es el máximo permitido para el Proxy LCP. Si el valor del mensaje de Proxy LCP procedente de un LAC es mayor que el MRU configurado en el LNS, L2TP intentará renegociar el LCP con un MRU igual al MRU configurado sin cambiar otras opciones LCP del LAC.

Configuración de túneles de capa 2

Para configurar L2T:

1. Acceda a la función de túnel de capa 2 mediante el mandato **feature**.

```
Config> feature layer-2-tunneling
Layer-2-Tunneling config>
```

2. Habilite L2TP, L2F y PPTP, según convenga.

```
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 tiene que ser estrictamente un LAC, L2F NAS o PPTP PAC, no es necesario que añada ninguna red L2T. Debe definir una red L2T para cada conexión PPP con 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 túneles L2TP, L2F o PPTP.

      Para configurar un túnel L2TP mediante una lista local 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 la creación de túneles de “reino” en la forma “user@lns.org.”

      Puede establecer que la autenticación y la autorización de túneles se realice en un servidor RADIUS concreto. Consulte “Utilización de la seguridad de autenticación, autorización y contabilidad (AAA)” en la publicación *Utilización y configuración de características.*

      Si está configurando un LNS y la autenticación de túneles está inhabilitada tanto en LAC como en LNS, no es necesario configurar perfiles de túneles.

      Para crear un túnel por nombre de usuario PPP en un LAC mediante una lista local 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. Configure la coincidencia de nombres de sistema principal remoto para los túneles de entrada, si es necesario.

   Observe que en casos de conexiones de marcación de cliente, habitualmente este paso no es necesario. Utilice esta opción cuando una conexión deba utilizar una red específica.

   Presuponiendo 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 de nombres de sistema principal remoto, utilice los siguientes mandatos:

```
Config> net 10
     L2TP 10> set any-remote-hostname
```

4. Configure llamadas salientes 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 está configurado para hacer una llamada RDSI a petición de línea conmutada 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. Establezca el nombre de autenticación en el caso de que el dispositivo LNS se autentique. Hay otros indicadores de mandatos que no aparecen en este ejemplo. Si desea obtener más detalles al respecto, consulte “Configuración de la autenticación PPP” en el capítulo “Utilización de las interfaces del protocolo punto a punto” de la publicación *Software de Access Integration Services Guía del usuario.*

b. Añada usuarios a autenticar en el LNS. Hay otros indicadores de mandatos que no aparecen en este ejemplo. Consulte Add en el capítulo “El proceso y los mandatos CONFIG (CONFIG - talk 6)” de la publicación *Software de Access Integration Services Guía del usuario* si desea obtener una descripción de la sintaxis de mandatos y de las opciones.

Configuración 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. Utilizado para efectuar la llamada física.

5. Configure los clientes de direccionador L2T. El siguiente ejemplo muestra una conexión directa L2TP mediante la función de cliente de direccionador L2TP. Esta conexión se establece en una sola dirección y está basada en peticiones.

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** — Establezca el nombre de autenticación en el caso de que el dispositivo cliente se autentique. Hay otros indicadores de mandatos que no aparecen en este ejemplo. Si desea obtener más detalles al respecto, consulte “Configuración de la autenticación PPP” en la publicación *Software de Access Integration Services Guía del usuario*

.

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 a autenticar en el LNS. Hay otros indicadores de mandatos que no aparecen en este ejemplo. Si desea obtener más detalles al respecto, consulte “el mandato Config **add**” en la publicación *Software de Access Integration Services Guía del usuario.*

6. Configure los diversos parámetros de la función L2T mediante los mandatos **set** y **enable**, si lo desea.

```
Layer-2-Tunneling Config>set ?
Layer-2-Tunneling Config>enable ?
```

7. Configure los parámetros PPP para todas las redes L2 que se hayan definido para entrada y especifique *any* como nombre de sistema principal de túnel de entrada mediante el mandato encapsulator, si lo desea.

```
Layer-2-Tunneling Config>encapsulator
PPP-L2TP Config>
```

   Cuando haya finalizado de configurar PPP, entre **exit** para volver al entorno de configuración de la función L2T.

Capítulo 25. Configuración y supervisión de los protocolos de túnel de capa 2

Este capítulo describe la configuración de túneles de capa 2 (L2T) y sus mandatos operativos. L2T consta del protocolo de túnel de capa 2 (L2TP), del protocolo de reenvío de capa 2 (L2F) y del protocolo de túnel punto a punto (PPTP). Las secciones de este capítulo son:

- "Acceso al indicador de configuración de la interfaz de L2T"
- "Mandatos de configuración de la interfaz de túneles L2"
- "Acceso al indicador de configuración de la función de túneles L2" en la página 419
- "Mandatos de configuración de la función de túnel L2" en la página 419
- "Acceso al indicador de supervisión de túneles L2" en la página 424
- "Mandatos de supervisión de túneles L2" en la página 425

Acceso al indicador de configuración de la interfaz de L2T

Para acceder al indicador de configuración de la interfaz de 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 420).
3. Entre **n** *núm_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 de túneles L2

La Tabla 49 resume los mandatos de configuración de la interfaz de L2T. Entre estos mandatos en el indicador `L2T Config n>` (donde *n* es el número de red).

Tabla 49. Mandatos de configuración de la interfaz de túneles L2

Mandato	Función
? (Ayuda)	Visualiza todos los mandatos disponibles para este nivel de mandato, o lista las opciones de mandatos específicos (si es que están disponibles). Consulte "Obtención de ayuda" en la página xxv.
Disable	Inhabilita las llamadas salientes.
Enable	Habilita las llamadas salientes.
Encapsulator	Le permite configurar los parámetros PPP de la interfaz L2T. **Nota:** La opción encapsulator sólo está disponible si una interfaz tiene un nombre de sistema principal remoto configurado.
List	Visualiza información sobre la interfaz L2T.
Set	Le permite establecer varios parámetros de interfaz L2T.
Exit	Hace volver al nivel de mandato anterior. Consulte "Salida de un entorno de nivel inferior" en la página xxv.

Disable

Utilice el mandato **disable** para inhabilitar llamadas salientes del concentrador de acceso de 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 de L2TP (LAC). Este mandato sólo se puede utilizar 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 PPP de la interfaz L2T.

Sintaxis: encapsulator

Este mandato está disponible sólo cuando se ha configurado un nombre de sistema principal remoto. Si desea obtener una lista de los mandatos disponibles en el indicador `ppp-L2tp config>`, consulte “Encapsulator” en la página 422.

List

Utilice el mandato **list** para visualizar el estado de los diversos parámetros de configuración de la 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

any-remote-hostname
Borra el nombre del sistema principal remoto de salida e inhabilita la comparación de nombres de sistema principal remoto de entrada de esta red.

connection-direction [inbound] o [outbound] o [both]
Especifica si se puede puede iniciar la conexión mediante el igual (inbound), el dispositivo local (outbound) o mediante ambos el igual y el dispositivo local (both) de esta red. Si especifica both, no podrá especificar cero como tiempo de inactividad.

Valor por omisión: inbound

idle-time *segundos*
Especifica los segundos de inactividad al cabo de los cuales los túneles L2 desconectarán la sesión de túnel en esta red. Cero indica que el túnel es fijo y que no debe desconectarse.

Valores válidos: 0 a 1024

Valor por omisión: 0

remote-hostname *nombre_de_sistema_principal*
Especifica el nombre de sistema principal del túnel del igual.

En el caso de un túnel de salida, el nombre de sistema principal especifica un perfil de túnel configurado en el subsistema AAA. Debe ser el nombre del sistema principal de túnel que el igual utiliza para identificarse a sí mismo.

En el caso de un túnel de entrada, sólo los iguales de túnel que se identifican a sí mismos con este nombre de sistema principal se pueden conectar a esta interfaz.

Valores válidos: Cualquier nombre de 1 a 64 caracteres ASCII

Valor por omisión: *Nombre*

Acceso al indicador de configuración de la función de túneles L2

Para acceder al indicador de configuración de la función de túnel L2:

1. Entre **talk 6** en el indicador OPCON (*).
2. Entre **feature layer-2-tunneling** en el indicador `Config>`.

Mandatos de configuración de la función de túnel L2

La Tabla 50 resume los mandatos de configuración de la función de túnel L2 y el resto de esta sección describe dichos mandatos. Entre estos mandatos en el indicador `Layer-2-Tunneling Config>`.

Tabla 50 (Página 1 de 2). Mandatos de configuración de la función de túnel L2

Mandato	Función
? (Ayuda)	Visualiza todos los mandatos disponibles para este nivel de mandato, o lista las opciones de mandatos específicos (si es que están disponibles). Consulte “Obtención de ayuda” en la página xxv.
Add	Añade redes e iguales de túneles L2.
Disable	Inhabilita las funciones de túnel L2.
Enable	Habilita las funciones de túnel L2.

Tabla 50 (Página 2 de 2). Mandatos de configuración de la función de túnel L2

Mandato	Función
Encapsulator	Le permite configurar los parámetros PPP de todas las redes L2 que no están configuradas con un nombre de sistema principal remoto (ANY).
List	Visualiza información sobre la configuración de túneles L2.
Set	Le permite establecer almacenamientos intermedios, la ventana de recepción de llamadas y otros parámetros de túneles L2.
Exit	Hace volver al nivel de mandato anterior. Consulte “Salida de un entorno de nivel inferior” en la página xxv.

Add

Utilice el mandato **add** para añadir redes L2. Es obligatoria una red L2 para cada sesión PPP simultánea que acabe en este direccionador. El final de una sesión PPP con túnel es el punto final del LNS del túnel.

Sintaxis: add
L2-nets

L2-nets

Nota: Todo el mandato se puede entrar en minúsculas. El carácter inicial aparece en mayúsculas para mayor claridad.

Añade redes L2 a la configuración de túneles L2. Es obligatoria una red L2 para cada sesión PPP simultánea que deba finalizar en este direccionador. Si este direccionador se utiliza estrictamente como un LAC, no se necesitan redes L2 virtuales. Cuando se entra este mandato, se le solicita el número de redes adicionales y si desea añadir direcciones IP no numeradas para cada red L2.

El número de redes adicionales hace referencia al número de redes que se añaden de manera automática en este momento. Estas redes se suman a las redes L2 que ya existen.

Al añadir direcciones IP no numeradas para cada red L2, se añaden de manera automática entradas IP no numeradas a la tabla de direccionamiento de cada una de las redes L2. Las direcciones IP no numeradas son el modo de operación preferente. Si necesita direcciones numeradas para las redes L2, las puede alterar en el entorno de configuración del protocolo IP (consulte el capítulo titulado “Configuring IP” de la publicación *Configuración y supervisión de protocolos - Manual de consulta Volumen 1*).

Disable

Utilice el mandato **disable** para inhabilitar las funciones de túnel L2.

Sintaxis: disable call-rcv-window
fixed-udp-source-port
force-chap-challenge
hiding-for-pap-attributes
L2f
L2tp
pptp
proxy-auth
proxy-lcp
tunnel-auth

call-rcv-window
Los túneles L2 pueden poner en cola paquetes para cada llamada a fin de llevar a cabo el control de secuencia y de congestión. Cada llamada dispone de su propia ventana, que es el número de paquetes que se pueden enviar antes de que se reciba un ACK. La inhabilitación de *call-rcv-window* desactiva el control de flujo y las secuencias de todas las sesiones. Ello puede ser conveniente cuando se sabe que una conexión entre el LAC y el LNS es de gran calidad, dispone de suficiente ancho de banda y no es propensa a la reordenación de paquetes.

fixed-udp-source-port
Autoriza mediante un puerto UDP fijo. Si inhabilita este parámetro deberá configurar filtros de Seguridad IP entre el LAC y el LNS por dirección IP.

force-chap-challenge
Inhabilita el reintento de LNS CHAP de un cliente. Es necesario que inhabilite el reintento de CHAP si el cliente PPP tiene problemas con los reintentos CHAP.

hiding-for-pap-attributes
Inhabilita el cifrado de información Proxy PAP entre el LAC y 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 autenticación por proxy PPP del LAC a LNS.

proxy-lcp
Inhabilita el envío de información LCP del LAC a LNS.

tunnel-auth
Inhabilita la autenticación de iguales de túneles basada en un secreto compartido de este direccionador.

Enable

Utilice el mandato **enable** para habilitar las funciones de túnel L2.

Sintaxis:

enable
- fixed-udp-source-port
- force-chap-challenge
- hiding-for-pap-attributes
- L2f
- L2tp
- pptp
- proxy-auth
- proxy-lcp
- tunnel-auth

fixed-udp-source-port
La habilitación de este parámetro le permite configurar filtros de Seguridad IP por puerto UDP para túneles L2 de manera que puede cifrar o autenticar fácilmente tráfico de túneles L2. Establece el puerto UDP en 1701 para L2TP.

force-chap-challenge
Habilita el reintento de CHAP de LNS de un cliente aunque el LNS reciba un CHAP de proxy. Esto es preferible desde el punto de vista de la seguridad, en

el caso de que se sepa que el cliente puede manejar dicho reintento sin problemas.

hiding-for-pap-attributes
Habilita el cifrado de la información Proxy PAP entre el LAC y LNS.

L2f Habilita L2F en este direccionador.

L2tp
Habilita L2TP en este direccionador.

pptp
Habilita PPTP en este direccionador.

proxy-auth
Habilita el envío de autenticación por proxy PPP del LAC a LNS.

proxy-lcp
Habilita el envío de información LCP del LAC a LNS.

tunnel-auth
Habilita la autenticación de iguales de túneles basada en un secreto compartido de este direccionador.

Encapsulator

Utilice el mandato **encapsulator** para acceder al indicador `ppp-L2tp config>` a fin de configurar los parámetros PPP de todas las interfaces de túneles de capa 2 que estén configuradas como de entrada y especificar *any* como nombre de sistema principal remoto.

Sintaxis: encapsulator

List

Utilice el mandato **list** para visualizar el estado de los diversos parámetros de configuración de túneles L2.

Sintaxis: list

```
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 túneles L2.

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 de túneles L2 internos solicitados. Si no hay suficiente memoria para satisfacer la petición, sólo estará disponible una parte de los almacenamientos intermedios en el momento del rearranque. Para confirmar la cantidad de memoria mientras L2T está activo, utilice el mandato **memory** (consulte “Memory” en la página 428).

Valores válidos: 1 a 1000

Valor por omisión: 200

call-rcv-window

Especifica el número de paquetes a utilizar como ventana de recepción y habilita call-rcv-window. Si el control de flujo está habilitado en el canal de datos, se deberá señalar un tamaño de ventana de recepción tanto para su utilización por parte del protocolo de este direccionador como para la comunicación con el igual mediante mensajes de arranque. El valor configurado es para todas las llamadas iniciadas para este direccionador. Cero significa sólo secuencia (sin control de flujo).

Valores válidos: 0 a 100

Valor por omisión: 0

error-check-period [seconds]
Especifica el periodo de sondeo de errores de hardware del LAC. Cada periodo de sondeo generará un mensaje de notificación de errores de WAN transmitido del LAC a LNS. El rango es de 60 a 65000 segundos.

Valor por omisión: 120 segundos.

host-lookup-password
Especifica el secreto compartido para la autorización de túneles RADIUS. Debe coincidir con el secreto configurado en el servidor.

Valor por omisión: Ninguno.

local-hostname
Especifica la cadena de caracteres del nombre de sistema principal que identifica el direccionador local y que se envía en mensajes de configuración de túneles.

Valor por omisión: IBM

max-calls
Especifica el número máximo de llamadas en todos los túneles que pueden estar activas 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 se vuelve a transmitir un paquete L2TP en el canal de control antes de que la sesión o el túnel se declaren inactivos y concluyan.

Valores válidos: 2 a 100

Valor por omisión: 6

tunnel-rcv-window
Especifica el tamaño de ventana de recepción L2TP para el transporte de conexiones de control de confianza. Dicho transporte transmite y recibe los mensajes necesarios para la configuración, el desmantelamiento y el mantenimiento de túneles o sesiones.

Valores válidos: 1 a 100

Valor por omisión: 4

Acceso al indicador de supervisión de túneles L2

Para acceder al indicador de supervisión de túneles L2:

1. Entre **talk 5** en el indicador OPCON (*).
2. Entre **feature layer-2-tunneling** en el indicador GWCON (+).

Mandatos de supervisión de túneles L2

Esta sección resume y, a continuación, describe los mandatos de supervisión de túneles L2. Entre los mandatos en el indicador `Layer-2-Tunneling Console>`.

La Tabla 51 resume los mandatos de supervisión de túneles L2.

Tabla 51. Mandatos de supervisión de túneles L2

Mandato	Función
? (Ayuda)	Visualiza todos los mandatos disponibles para este nivel de mandato, o lista las opciones de mandatos específicos (si es que están disponibles). Consulte "Obtención de ayuda" en la página xxv.
Call	Visualiza estadísticas e información sobre cada llamada en proceso.
Kill	Finaliza un túnel de manera inmediata.
Memory	Visualiza la asignación y el uso del almacenamiento intermedio de túneles L2.
Start	Inicia un túnel con otro igual.
Stop	Detiene un túnel y permite que cada igual lleve a cabo cualquier tarea de administración necesaria.
Tunnel	Visualiza estadísticas e información de cada túnel existente.
Exit	Hace volver al nivel de mandato anterior. Consulte "Salida de un entorno de nivel inferior" en la página xxv.

Call

Utilice el mandato **call** para visualizar estadísticas e información de llamadas.

Sintaxis: call
errors
physical-errors
queue
state
statistics

errors
Visualiza los errores de transmisión generales 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
El identificador local asociado a esta llamada.

Serial #
El número utilizado para el registro cronológico de esta llamada.

ACK-timeout
El número de veces que se ha recibido del igual una notificación de tiempo de espera excedido.

Dropped pkts
El número de paquetes que se han declarado perdidos para esta llamada. Son los paquetes que se deberían haber recibido, pero que el igual ha señalado como perdidos.

physical-errors
Visualiza errores de datos que se han producido en las llamadas.

Ejemplo:

Mandatos de supervisión de túneles L2 (talk 5)

```
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 |
```

CallID
El identificador local asociado a esta llamada.

Serial #
El número utilizado para el registro cronológico de esta llamada.

CRC Errors
El número de paquetes en los que no ha coincidido el CRC.

framing errors
El número de paquetes con un error de trama.

HW overrun
El número de veces que se ha producido un desbordamiento de hardware.

buffer overrun
El número de veces que se ha producido un desbordamiento de almacenamiento intermedio

timeout errors
El número de veces que una interfaz ha excedido el tiempo de espera.

alignment
El número de veces que se ha producido un error de alineación.

time since updated
El tiempo que ha transcurrido desde el último sondeo de errores.

queue
Visualiza información sobre la cola de 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
El identificador local asociado a esta llamada.

Serial #
El número utilizado para el registro cronológico de esta llamada.

Tx Win
La ventana de recepción máxima para datos del igual.

Rx Win
La ventana de transmisión máxima local.

Ns El siguiente número de secuencia de paquetes a enviar para esta llamada.

Nr El siguiente número de secuencia de paquete que se espera recibir para esta llamada.

Rx Q
El número actual de paquetes en la cola de recepción.

Tx Q
El número actual de paquetes en la cola de transmisión.

priority
El número de paquetes PPP de prioridad que esperan a ser transmitidos por L2TP.

out Q
El 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
El identificador local asociado a esta llamada.

Serial #
El número utilizado para el registro cronológico de esta llamada.

Net #
El número de dispositivo asociado a esta llamada. En el caso de una llamada LNS, es la red L2. En el caso de una llamada LAC, es el dispositivo PPP que ha recibido la llamada inicial.

State
El estado de llamada actual. Los estados de llamada válidos son:

Established
Preparado para tráfico de red con túnel.

Idle
La llamada está desocupada.

Wait Cs Answer
Esperando que el enlace de comunicación se abra.

Wait Reply
Esperando respuesta del igual.

Wait Tunnel
Esperando establecimiento del túnel.

Time since chg
El tiempo que ha transcurrido desde el último cambio de estado.

PeerID
El ID de llamada del igual.

TunnelID
El túnel local asociado a esta llamada.

statistics
Visualiza estadísticas sobre la transmisión de datos de cada llamada.

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
El identificador local asociado a esta llamada.

Serial #
El número utilizado para el registro cronológico de esta llamada.

Tx Pkts
El número de paquetes transmitidos para esta llamada.

Tx Bytes
El número de bytes transmitidos para esta llamada.

Rx Pkts
El número de paquetes recibidos para esta llamada.

Rx Bytes
El número de bytes recibidos para esta llamada.

RTT
El tiempo de ida y vuelta calculado actualmente para esta llamada.

ATO
El tiempo de espera de adaptación calculado actualmente para esta llamada.

Kill

Utilice el mandato **kill** para finalizar de manera inmediata un túnel. Este mandato libera todos los recursos locales de un túnel, con lo que se fuerza la finalización de la conexión. No se envía ninguna notificación de la finalización del túnel al igual.

Nota: Utilice este mandato sólo si el mandato **stop** no puede finalizar un túnel.

Sintaxis: kill
tunnel *id_túnel*

tunnel *id_túnel*
Especifica el túnel a finalizar.

Memory

Utilice el mandato **memory** para visualizar el nivel de utilización de memoria actual del L2TP.

Sintaxis: memory

Ejemplo:

```
Layer-2-Tunneling Console> mem
Number of layer-2-tunneling buffers: Requested = 2000, Total = 1200, Free
= 1000
```

En este ejemplo, se han configurado 2000 almacenamientos intermedios, pero sólo se han podido asignar 1200. En este momento, 200 están en uso y 1000 están libres.

Start

Utilice el mandato **start** para iniciar un túnel con otro igual.

Sintaxis: start
(ningún parámetro solicitará un nombre de sistema principal)
tunnel *nombre_de_sistema_principal*

nombre_de_sistema_principal
El nombre del sistema principal con el que L2T establece el túnel.

Stop

Utilice el mandato **stop** para detener un túnel. Se llevan a cabo las operaciones de limpieza necesarias antes de que finalice el túnel.

Sintaxis: stop
tunnel *id_túnel*

tunnel *id_túnel*
Especifica el túnel a finalizar.

Tunnel

Utilice el mandato **tunnel** para visualizar estadísticas e información sobre todos los túneles.

Sintaxis: tunnel
call
errors
peer
queue
state
statistics
transport

calls
Visualiza todos los túneles y el estado de cada llamada dentro de cada túnel.

errors
Visualiza los errores que se han producido 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
El identificador local asociado a este túnel.

Type
El tipo de protocolo de túnel que se está utilizando.

ACK-timeouts
El número de veces que se ha recibido del igual una notificación de tiempo de espera excedido.

peer
Visualiza los túneles y los iguales asociados a los túneles.

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
El identificador local asociado a un túnel.

Type
El tipo de protocolo de túnel que se está utilizando.

Peer ID
El identificador de túnel asignado a este túnel del igual.

Peer Hostname
El nombre del sistema principal tal y como aparece en la base de datos local.

Mandatos de supervisión de túneles L2 (talk 5)

queue

Visualiza información sobre la cola de 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
El identificador local asociado a un túnel.

Type
El tipo de protocolo de túnel que se está utilizando.

Rx Win
El número local máximo de paquetes que constituyen la ventana de recepción.

Tx Win
El número máximo de paquetes del igual que constituyen la ventana de recepción.

Ns El número de secuencia del siguiente paquete a enviar.

Nr El número de secuencia del siguiente paquete a recibir.

Rx Q
El número de paquetes que se hallan actualmente en la cola de recepción.

Tx Q
El número de paquetes que se hallan actualmente 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
El identificador local asociado a un túnel.

Type
El tipo de protocolo de túnel que se está utilizando.

Peer ID
El identificador de túnel asignado a este túnel del igual.

State
El estado de túnel actual. Los estados de túnel válidos son:

Established
El túnel se ha establecido.

Idle
El túnel está desocupado.

Wait Ctrl Reply
El sistema principal está esperando una respuesta del igual.

Wait Ctrl Conn
El sistema principal está esperando una indicación de conexión.

Time since chg
El tiempo que ha transcurrido desde el último cambio de estado.

 # Calls
El número de llamadas activas en este túnel.

Flags
Los indicadores utilizados para controlar los mensajes de conexión de este túnel.

statistics
Visualiza las estadísticas asociadas a 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
El identificador local asociado a un túnel.

Type
El tipo de protocolo de túnel que se está utilizando.

Tx Pkts
El número de paquetes transmitidos.

Tx Bytes
El número de bytes transmitidos.

Rx Pkts
El número de paquetes recibidos.

Rx Bytes
El número de bytes recibidos.

RTT
El tiempo de ida y vuelta calculado actualmente para mensajes de conexión de control de túneles.

ATO
El tiempo de espera de adaptación calculado actualmente para mensajes de conexión de control de túneles.

transport
Visualiza información referente a UDP sobre 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
El identificador local asociado a un túnel.

Type
El tipo de protocolo de túnel que se está utilizando.

Peer IP address
La dirección IP del igual para este túnel.

UDP Src
El puerto UDP de origen para este túnel.

Mandatos de supervisión de túneles L2 (talk 5)

UDP Dest
El puerto UDP de destino para este túnel.

Capítulo 26. Utilización de la conversión de direcciones de red (NAT)

La conversión de direcciones de red (NAT) y su extensión, la conversión de puertos y direcciones de red (NAPT), pueden ampliar el número de direcciones IP disponibles para una organización y pueden evitar que los usuarios de la red pública conozcan algunas de las direcciones de la red privada. NAT funciona utilizando direcciones públicas IP para que representen direcciones privadas IP.

Las direcciones públicas IP son las direcciones válidas de sistemas principales en la red pública IP y deben ser exclusivas dentro de la red pública. Si la red pública es Internet, las direcciones IP públicas deben ser direcciones de Internet exclusivas suministradas por el Network Information Center (NIC).

El direccionador conoce las direcciones privadas, pero la red pública no las conoce. Las direcciones de cada red privada deben ser exclusivas; de todos modos, la misma dirección se puede duplicar en dos redes privadas diferentes. Las direcciones privadas se asignan a sistemas principales dentro de redes apéndice. Las redes apéndice son redes que tienen acceso a la red pública a través de un solo direccionador.

NAT amplía el número de direcciones IP disponibles de diversas maneras:

- Permite que cada dirección pública represente varias direcciones privadas mediante la rotación del uso de las direcciones públicas.
- Permite la duplicación de direcciones en la medida en que cada dirección duplicada se utilice en una red privada diferente.
- Permite que el administrador de la red utilice las direcciones IP de las redes privadas, en lugar de las direcciones NIC que se están convirtiendo en recursos limitados.

La utilización de direcciones privadas oculta también éstas frente al mundo exterior. Esta función de NAT lo hace útil como cortafuegos para evitar que se conozcan las direcciones privadas.

Importante: Tal y como se señala en la sección 5.4 del documento borrador de Internet que define NAT, “cualquier aplicación que transporte (y utilice) la dirección IP (y el puerto TCP/UDP, en el caso de la NAPT) dentro de la aplicación no operará a través de NAT...”. Se debe tener en cuenta que DLSw y XTP toman decisiones basadas en las direcciones IP de punto final — concretamente deciden cuál es el asociado que dispone de la dirección más alta. Como la aplicación (DLSw o XTP) que está funcionando a través de NAT cree que su dirección es la dirección privada y la aplicación asociada del otro direccionador cree que la dirección de la aplicación es la dirección pública, se pueden tomar decisiones incorrectas.

La Figura 41 en la página 434 muestra el plano de una estación de trabajo en una red apéndice. En dicho ejemplo, la red apéndice consta de una subred IP que tiene la dirección IP 10.33.96.0 con la máscara de subred 255.255.255.0.

Utilización de la conversión de direcciones de red (NAT)

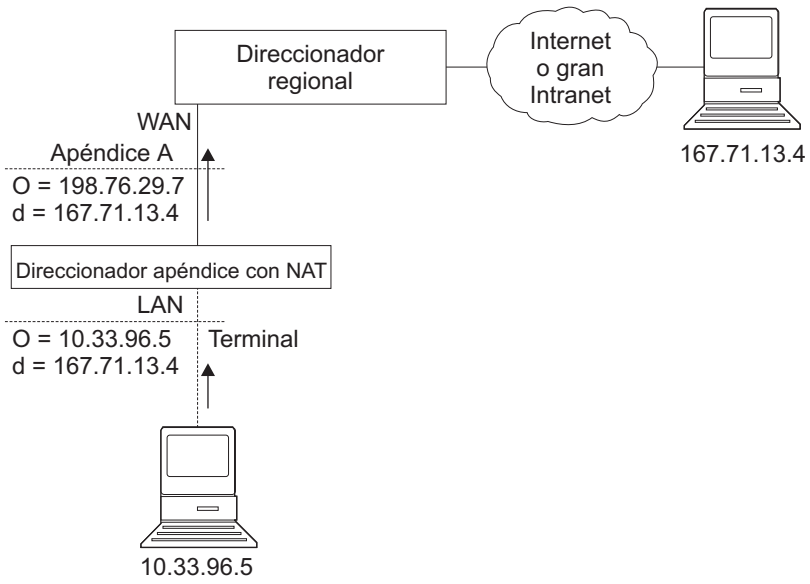


Figura 41. Red en la que se ejecuta NAT

Para utilizar NAT, el administrador de la red asigna una o más direcciones IP públicas a una agrupación de direcciones públicas en el 2212 y asigna una dirección IP privada a cada estación de trabajo de la red apéndice. Las direcciones IP públicas se asignan a una *agrupación de reserva* y las direcciones IP privadas se asignan al *rango de conversión*.

La función NAT enlaza en primer lugar la dirección privada de una estación de la red privada a una de las direcciones públicas. Enlazar significa que todos los paquetes que posean dicha dirección privada se convertirán a dicha dirección IP pública cuando el paquete salga. Los paquetes de entrada tiene la dirección IP pública como destino. NAT reconoce la dirección pública, la convierte en la dirección IP privada y reenvía el paquete. Después de que se detenga el tráfico, el enlace se mantiene hasta que un temporizador que el usuario puede establecer excede el tiempo de espera. En este momento, NAT finaliza el enlace y pone a disposición la dirección pública para que se pueda volver a utilizar.

En este ejemplo, se transmite un paquete desde la dirección de origen privada de envío 10.33.96.5 a una dirección de destino de Internet, 167.71.13.4. La función NAT del 2212 convierte la dirección privada 10.33.96.5 en la dirección pública 198.76.29.7. Esta conversión oculta a la red pública la dirección privada 10.33.96.5, 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, en cambio, 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 en la dirección privada 10.33.96.5 y reenvía los paquetes.

Conversión de puertos y direcciones de red

NAPT se puede utilizar sólo para tráfico TCP y UDP. En NAPT, varias direcciones privadas pueden utilizar una única dirección pública simultáneamente. Mientras que NAT correlaciona una dirección pública con una dirección privada, NAPT correlaciona la dirección pública NAPT ***y*** el número del puerto público con una dirección privada y un número de puerto privado. Sólo se puede configurar una dirección NAPT para cada agrupación de direcciones públicas.

NAPT se configura fácilmente especificando una dirección pública o una interfaz de direcciones dinámicas (que esté utilizando PPP/IPCP para recuperar una dirección pública) que se utilizará para tráfico NAPT. La ventaja de NAPT es que puede habilitar una dirección de la agrupación de direcciones IP públicas para que ofrezcan soporte a muchas direcciones IP privadas de manera simultánea.

Correlaciones de direcciones estáticas

Es probable que en ocasiones desee configurar una estación o servidor en la red privada al que se puede acceder directamente desde la red pública. En ese caso, deberá llevar a cabo una correlación estática de la dirección privada de la estación con una dirección pública concreta. Todos los mensajes que salen de la dirección privada se convierten a la dirección pública designada y todos los mensajes que entran para la dirección pública designada se reenvían de manera automática a la dirección privada asociada. Existen dos tipos de correlaciones de direcciones estáticas: NAT y NAPT.

Correlación de direcciones estáticas NAT

En una correlación NAT, todos los protocolos IP pueden acceder al sistema principal. El siguiente 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 incorpore un puerto privado conocido públicamente. En el caso de correlación de direcciones estáticas, se debe configurar una dirección pública NAPT. Por ejemplo, para configurar un sistema principal Telnet en la dirección privada 10.1.1.1 para utilizar la dirección pública NAPT 9.67.1.2, la correlación estática se configuraría del siguiente modo:

Dirección privada	10.1.1.1
Puerto privado	23
Dirección NAPT pública	9.67.1.2
Puerto público	23

Los puertos públicos y privados se correlacionan con el puerto 23, que es el puerto conocido públicamente para Telnet. Ahora, si el administrador también dispone de un servidor FTP (dirección conocida públicamente 21) en la misma dirección privada 10.1.1.1 a correlacionar con la dirección pública NAPT 9.67.1.2, dicha correlación tendrá un aspecto similar a éste:

Dirección privada	10.1.1.1
Puerto privado	21
Dirección NAPT pública	9.67.1.2
Puerto público	21

El servidor de la dirección 10.1.1.1 tiene la misma dirección pública NAPT (9.67.1.2) para ambas aplicaciones pero NAPT las puede diferenciar utilizando números de puerto diferentes (23 y 21). De todos modos, NAPT no puede diferenciar dos servidores que utilizan la misma dirección pública NAPT y que tienen el mismo número de puerto y de aplicación. Por ejemplo, si la dirección pública NAPT y el puerto conocido públicamente son los mismos para 10.1.1.3 puerto 21 que para 10.1.1.1 puerto 21, NAPT no puede indicar si debe enviar tráfico FTP entrante al servidor 10.1.1.3 o al servidor 10.1.1.1. Para configurar más de un servidor con las mismas dirección NAPT y aplicación, deberá utilizar un puerto que no sea el puerto conocido públicamente en el servidor (por ejemplo, iniciar el daemon FTP en el puerto 200).

Establecimiento de filtros de paquetes y de reglas de control de acceso para NAT

Además de identificar el rango de direcciones privadas que NAT o NAPT deben convertir, el administrador debe configurar filtros de paquetes y reglas de control de acceso para IP en el 2212. La configuración de NAT requiere que se configuren un filtro de paquetes de entrada y uno de salida en la interfaz que esté conectada a la red pública. Es necesario que configure una o más reglas de control de acceso en el filtro de paquetes de entrada y una o más reglas de control de acceso en el filtro de paquetes de salida. Las reglas de control de acceso del filtro de entrada dejan pasar a NAT los paquetes de entrada que tengan definidas las direcciones públicas adecuadas. Las reglas de control de acceso del filtro de salida dejan pasar a NAT los paquetes de salida que tengan definidas las direcciones privadas adecuadas.

Las reglas de control de acceso que se aplican para NAT disponen de los tipos de reglas de control de acceso ***I*** (inclusivo) y ***N*** (NAT). Consulte el *Configuración y supervisión de protocolos - Manual de consulta, Vol. 1* para obtener más información sobre la configuración de controles de acceso IP.

Nota: NAT también se puede configurar junto con un túnel IPsec. Encontrará un ejemplo de dicha configuración en “Configuración de las normas del control de acceso de filtros de paquetes para el direccionador A” en la página 372.

Ejemplo: Configuración de NAT con filtros IP y reglas de control de acceso

Este ejemplo le muestra cómo configurar NAT para el direccionador apéndice en la red que aparece en la Figura 42 en la página 437. Consulte Capítulo 27, “Configuración y supervisión de la conversión de direcciones de red” en la página 441 si desea obtener una descripción de los mandatos.

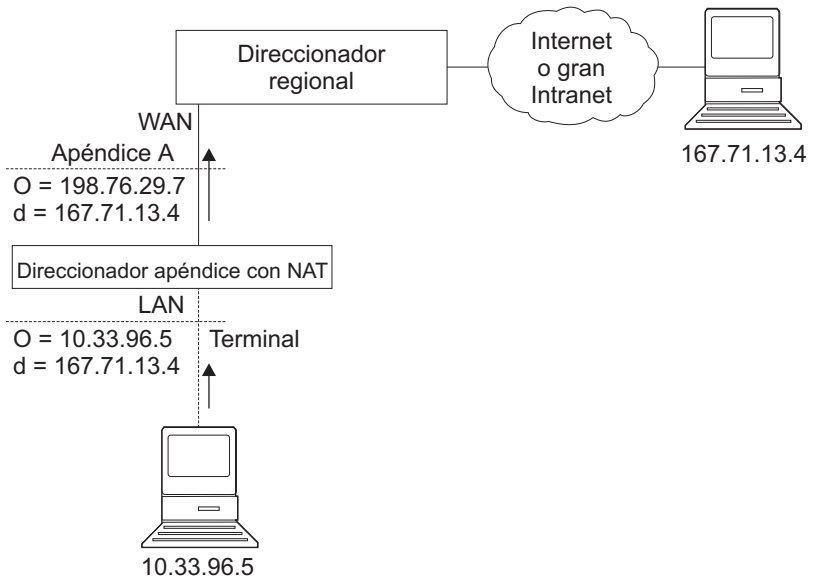


Figura 42. Red en la que se ejecuta NAT

Siga los pasos siguientes:

1. Configure agrupaciones de direcciones públicas para que NAT y NAPT las utilicen. Para hacerlo, 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, con lo que la agrupación está configurada para excluirlas. Los parámetros que se entran son: *dirección-pública, máscara, número-en-grupo, nombre y dirección-napt*. El valor 0.0.0.0 como dirección NAPT significa que ninguna de las direcciones de este grupo es la dirección NAPT. Utilice 0.0.0.0 como dirección NAPT de 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 deben convertir en pool1. Los parámetros que se entran son: *dirección-privada, máscara y nombre.*

   ```
   NAT config> translate 10.33.96.0 255.255.255.0 pool1
   ```

3. Configure las correlaciones estáticas para estaciones dentro de la red privada que deban estar correlacionadas permanentemente con una de las direcciones públicas. Los siguientes mandatos identifican una máquina (10.33.96.5) que recibirá cualquier tipo de tráfico desde la red pública. Una segunda máquina (10.33.96.4) es tanto un servidor Telnet como un servidor HTTP. Los parámetros son *dirección-privada, número-puerto-privado, dirección-pública y número-puerto-público.* Observe que la dirección NAPT para pool1 se utiliza como la dirección pública para el sistema principal que está 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.

   ```
   NAT config> enable NAT
   ```

5. Cree dos filtros de paquete IP para que IP deje pasar paquetes a NAT. Se trata de filtros de paquetes de entrada y de salida para la interfaz 0, que es la interfaz 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. Los paquetes recibidos en la interfaz pública (red 0) que están destinados para una dirección de la agrupación de direcciones públicas reservadas de NAT se deben dejar pasar a NAT. NAT sustituirá la dirección pública (y el puerto público si el paquete está destinado a la dirección NAPT) con la dirección privada correcta (y el puerto privado si el paquete está destinado a la dirección NAPT). La dirección 0.0.0.0 y la máscara del origen de Internet indican que todas las direcciones de origen de la red pública pasará 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 definido en pool1. Si la dirección del paquete que se ha dejado pasar a NAT se encuentra en el rango definido en la regla de control de acceso pero no es uno de los que forman parte de la agrupación de direcciones, NAT devuelve el paquete a IP sin modificarlo.

7. Si desea que el direccionador pase paquetes que no cumplen con la regla de control de acceso, en lugar de eliminarlos, puede crear una regla comodín de control de acceso. El siguiente ejemplo muestra este tipo de regla de control de acceso:

```
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 reenvíen desde la interfaz 0 de red y que disponen de una dirección de origen en la red privada son identificados a fin de que IP los pueda pasar a NAT. NAT sustituye la dirección privada por una de la 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 paquete, al igual que con el filtro *in-0*, puede añadir una regla comodín de control de acceso inclusivo como última regla de control de acceso si prevé reenviar paquetes que no cumplen con la regla de control de acceso.

9. Puede utilizar el mandato **list packet-filter** *nombre-filtro* desde el indicador `IP Config>` para comprobar la precisión y la secuencia de las reglas de control de acceso en cada filtro de paquete.
10. Habilite los controles de acceso para IP.

    ```
    IP Config> set access-control on
    ```

11. Restablezca IP y NAT mediante talk 5. Hasta ahora, se han efectuado modificaciones en la configuración del direccionador pero dichos cambios no han afectado al direccionador. Los mandatos de restablecimiento (reset) de IP y NAT hacen que el direccionador lea en la nueva configuración y que ejecute con las reglas definidas en la configuración.

    ```
    NAT> reset NAT
    IP> reset IP
    ```

Utilización de la conversión de direcciones de red (NAT)

Capítulo 27. Configuración y supervisión de la conversión de direcciones de red

Este capítulo describe los mandatos de configuración y de supervisión de la conversión de direcciones de red (NAT) y consta de las siguientes secciones:

- "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 448
- "Mandatos de supervisión de la conversión de direcciones de red" en la página 448

Acceso al entorno de configuración de la conversión de direcciones de red

Para acceder al entorno de configuración NAT, entre el mandato siguiente 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 describe los mandatos de configuración de la conversión de direcciones de red (NAT). Para configurar NAT, entre estos mandatos en el indicador `NAT config>`.

Tabla 52. Mandatos de configuración de NAT

Mandato	Función
? (Ayuda)	Visualiza todos los mandatos disponibles para este nivel de mandato, o lista las opciones de mandatos específicos (si es que están disponibles). Consulte "Obtención de ayuda" en la página xxv.
Change	Cambia agrupaciones de reserva de direcciones IP públicas, rangos de conversión de direcciones privadas y correlaciones estáticas.
Delete	Suprime agrupaciones de reserva de direcciones IP públicas, rangos de conversión de direcciones privadas y correlaciones estáticas.
Disable	Inhabilita NAT.
Enable	Habilita NAT.
List	Lista información sobre la configuración de NAT.
Map	Crea un enlace NAT o NAPT estático para una estación o servidor.
Reserve	Crea una agrupación de direcciones IP públicas y añade direcciones a dicha agrupación.
Reset	Hace que el direccionador lea en la configuración NAT y ejecute según las reglas NAT que se han configurado.
Set	Establece tiempos de espera.
Translate	identifica las direcciones IP privadas que se la agrupación de direcciones públicas NAT debe convertir.
Exit	Hace volver al nivel de mandato anterior. Consulte "Salida de un entorno de nivel inferior" en la página xxv.

Change

Utilice el mandato **change** para cambiar agrupaciones de reserva de direcciones IP públicas, rangos de conversión de direcciones IP privadas y correlaciones estáticas.

Sintaxis:

change reserve
translate
mappings

reserve *agrupaciones*
Proporciona indicadores que le permiten modificar las características de cualquiera de las agrupaciones de reserva de direcciones IP públicas (como, por ejemplo, direcciones IP y máscaras).

Valores válidos: Un número de índice para identificar la agrupación configurada. Dicho número se visualiza cuando se entra el mandato **list reserve pools**.

Valor por omisión: ninguno

translate *rangos*
Proporciona indicadores que le permiten modificar las características de cualquiera de los rangos de conversión de direcciones IP privadas (como, por ejemplo, direcciones IP y máscaras).

Valores válidos: Un número de índice para identificar el rango de conversión configurado. Dicho número se visualiza cuando se entra el mandato **list translate**.

Valor por omisión: ninguno

mappings
Proporciona indicadores que le permiten modificar las características de cualquiera de las correlaciones de direcciones estáticas (como, por ejemplo, direcciones IP y puertos).

Valores válidos: Un número de índice para identificar la correlación configurada. Dicho número se visualiza cuando se entra el mandato **list mappings**.

Valor por omisión: ninguno

Delete

Utilice el mandato **delete** para suprimir agrupaciones de reserva de direcciones IP públicas, rangos de direcciones IP privadas y correlaciones.

Sintaxis:

delete reserve
translate
mappings

reserve *agrupaciones*
Proporciona indicadores que le permiten suprimir cualquiera de las agrupaciones de reserva de direcciones IP públicas.

Valores válidos: Un número de índice para identificar la agrupación configurada. Dicho número se visualiza cuando se entra el mandato **list reserve pools**.

Valor por omisión: ninguno

translate *rangos*
Proporciona indicadores que le permiten suprimir cualquiera de los rangos de conversión de direcciones IP privadas.

Valores válidos: Un número de índice para identificar el rango de conversión configurado. Dicho número se visualiza cuando se entra el mandato **list translate**.

Valor por omisión: ninguno

mappings
Proporciona indicadores que le permiten suprimir cualquiera de las correlaciones de direcciones estáticas.

Valores válidos: Un número de índice para identificar la correlación configurada. Dicho número se visualiza cuando se entra el mandato **list mappings**.

Valor por omisión: ninguno

Disable

Utilice el mandato **disable** para inhabilitar NAT. Puede inhabilitar NAT para que elimine paquetes que requieren conversión o puede inhabilitar NAT para que deje pasar paquetes que requieren conversión.

Sintaxis:

disable nat
drop
pass

drop
Inhabilita NAT para que elimine paquetes que requieren conversión.

pass Inhabilita NAT para que deje pasar paquetes que requieren conversión.

Enable

Utilice el mandato **enable** para habilitar NAT. Al habilitar NAT ya está preparada para ejecutarse pero no lo hará 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, los rangos de conversión de direcciones IP privadas, las correlaciones, los valores globales o toda la información de NAT.

Sintaxis:

list

reserve
- addresses
- pools

translate

mappings

global

all

En el ejemplo siguiente, el tiempo se visualiza en horas, minutos y segundos. La antigüedad de la entrada es el tiempo que ha transcurrido desde que la estrada se utilizó por última vez. Enlace significa que el tráfico está fluyendo entre estas dos direcciones. Los tiempos de espera determinan el tiempo que transcurrirá después de la última comunicación hasta que se elimine un enlace. Consulte el mandato **set** si desea obtener más información sobre 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 enlazar de manera estática un sistema principal o servidor de la red privada a un dirección pública. Este mandato, que se puede utilizar para configurar servidores de la red privada, establece una asociación cuando se arranca NAT que no cambia nunca.

Las correlaciones estáticas con el número de puerto privado o público 0 son correlaciones NAT; las que poseen otros valores de número de puerto son correlaciones NAPT.

Sintaxis:

map *dirección-privada número-puerto-privado dirección-pública número-puerto-público*

dirección privada

La dirección privada de la estación de trabajo.

Valores válidos: una dirección de sistema principal de Internet en un formato IP válido. Debe ser la dirección asignada a una estación en la red apéndice que requiere acceso permanente desde la red pública, como, por ejemplo, un servidor.

Valor por omisión: ninguno

número de puerto privado
El número de puerto TCP/UDP de la aplicación que se ejecuta en el dispositivo con la dirección privada. Si entra **0** se crea un enlace NAT y si entra otro valor se crea un enlace NAPT. Valores de puerto comunes 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 en el caso de una correlación NAPT y una dirección NAT en el caso de una correlación NAT.

Valores válidos: una dirección IP válida exclusiva de la red pública. La red pública puede ser Internet o una intranet, en función del diseño de la red.

Valor por omisión: ninguno

número de puerto público
El número de puerto de los paquetes que se deben convertir en la dirección pública. El valor 0 representa todos los puertos. Los valores comunes 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 dirección IP privada 10.11.12.200 acepta todo el tráfico de Internet; el servidor con dirección privada 10.11.12.199 es un servidor Telnet y un servidor 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. Se puede utilizar así mismo para añadir una interfaz IP dinámica a la agrupación de direcciones públicas.

Sintaxis:

reserve *dynamic [interface][dirección-pública][máscara][número-en-grupo] nombre [dirección-napt]*

Nota: Los valores que aparecen entre corchetes se visualizan ahora de manera opcional.

- Dynamic - Especifica si esta entrada es para un grupo de direcciones públicas o para una interfaz de direcciones dinámicas que recuperarán su dirección IP de una conexión PPP que está utilizando IPCP. Los valores válidos son *yes* (sí) o *no*. El valor por omisión es *no*. Si Dynamic=*yes* (sí), sólo deberá especificar la interfaz y el nombre. Si Dynamic=*no*, no deberá especificar la interfaz pero sí el resto de valores.

- Interface - Especifica la interfaz de direcciones dinámicas tal y como está configurada dentro de IP. Se puede especificar cualquier número de interfaz válido. El valor por omisión es cero.

dirección pública
La primera dirección IP pública en la secuencia de direcciones que componen este rango o grupo de la agrupación. Por ejemplo, si este grupo de la agrupación consta de 12 direcciones comprendidas en la secuencia que va desde 9.8.7.6 a 9.8.7.17, dicho valor es 9.8.7.6.

Nota: Para añadir otro rango de direcciones a la agrupación de direcciones públicas, utilice el mandato **reserve** independientemente para cada grupo, relacionando un grupo con otro mediante la utilización del mismo nombre de agrupación. Por ejemplo, las direcciones que van de 9.8.7.6 a 9.8.7.17 se pueden configurar en un grupo dentro de la pool1 y las direcciones que van de 9.8.7.1 a 9.8.7.3 se pueden configurar en otro grupo dentro de la misma agrupación. Por lo tanto, esta agrupación no configura ni utiliza las direcciones 9.8.7.4 y 9.8.7.5.

Valores válidos: una dirección IP válida que sea exclusiva de la red pública

Valor por omisión: ninguno

máscara
Una máscara para seleccionar bits de la dirección IP. La máscara, al igual que una dirección IP, tiene una longitud de 32 bits. Los unos (1) de la máscara seleccionan la parte de red o subred de la dirección. Los ceros (0) seleccionan la parte de 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 primeros dos 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 el grupo
Especifica el número de direcciones secuenciales, empezando por la *dirección-pública*, que se incluyen en el grupo. En el caso de las direcciones de 9.8.7.6 a 9.8.7.17, este valor es 12.

Valores válidos: 1 - el valor que la máscara IP pueda definir

Valor por omisión: ninguno

nombre
El nombre de la agrupación de reserva de direcciones públicas. Esta cadena debe coincidir con el nombre de la agrupación del mandato **translate** correspondiente.

Valores válidos: cualquier nombre, con un máximo de 16 caracteres imprimibles; los espacios en blanco iniciales y finales se ignoran.

Valor por omisión: ninguno

dirección napt
La dirección IP de la agrupación de direcciones públicas que la conversión de puertos y direcciones de red (NAPT) utilizará. Esta dirección se utiliza para tráfico TCP y UDP a fin de correlacionar varias direcciones privadas con la dirección NAPT según el número de puerto de protocolo. La utilización de NAPT es opcional. Si se utiliza, sólo puede haber una dirección NAPT por

cada agrupación de direcciones públicas. Si no existe ninguna dirección NAPT para una agrupación o grupo, entre el valor **0.0.0.0**. Sólo tiene que entrar una vez la dirección NAPT para la agrupación.

Valores válidos: una de las direcciones IP públicas. No debe estar incluida necesariamente en el rango de valores definidos en la agrupación de direcciones públicas pero sí que debe hallarse en la misma subred.

Valor por omisión: 0.0.0.0 (que significa sin 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 reiniciar NAT. Este mandato suprime todos los enlaces, libera toda la memoria utilizada por NAT y reinicia NAT según la configuración actual de Talk 6. Cuando se reinicia NAT no se interrumpe ningún otro componente del 2212.

Sintaxis:

reset n**at**

Tenga en cuenta que si NAT encuentra una configuración no válida, aparecerá un mensaje en ese sentido. Repase los mensajes NAT ELS para saber por qué ha fallado la inicialización.

Set

Utilice el mandato **set** para establecer tiempos de espera TCP y no TCP.

Sintaxis:

set t**cp**
n**ontcp**

tcp *timeout*
El tiempo que NAT mantiene un enlace TCP después de que el último mensaje pase entre las dos estaciones de trabajo enlazadas. Un enlace 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 45 días, aproximadamente)

Valor por omisión: 1440 minutos (24 horas)

nontcp *tiempo de espera*
El tiempo que NAT mantiene un enlace que no es TCP después de que el último mensaje haya pasado entre las dos estaciones enlazadas. Un enlace 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 45 días, aproximadamente)

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. Este mandato se debe entrar para cada rango de conversión que NAT deba conocer. Cualquier número de rangos de conversión puede utilizar una única agrupación de reserva de direcciones públicas.

Sintaxis:

t**ranslate** *Dirección-privada máscara nombre*

dirección privada
Cualquier sistema principal IP o dirección de subred que se deba convertir.

Valores válidos: una dirección en formato IP decimal con puntos válida. Cuando se realiza un AND con su máscara de subred, esta dirección identifica todas las direcciones de una subred apéndice. Una subred apéndice es una red que accede a la red pública sólo a través del direccionador.

Valor por omisión: ninguno

máscara
Valores válidos: La máscara de red o subred asociada con la red apéndice que debe ser convertida.

Valor por omisión: la 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, con un máximo de 16 caracteres imprimibles. Debe coincidir con un nombre de agrupación de direcciones públicas creado mediante 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>
```

Aparece el indicador NAT>.

Mandatos de supervisión de la conversión de direcciones de red

Esta sección describe los mandatos de supervisión de la Seguridad IP. Entre estos mandatos en el indicador NAT>.

Tabla 53. Mandatos de supervisión de NAT

Mandato	Función
? (Ayuda)	Visualiza todos los mandatos disponibles para este nivel de mandato, o lista las opciones de mandatos específicos (si es que están disponibles). Consulte “Obtención de ayuda” en la página xxv.
List	Lista información sobre NAT.
Reset	Hace que el direccionador lea en la configuración NAT y ejecute según las reglas de acceso NAT que se han configurado. NAT no afecta al funcionamiento del direccionador hasta que se entra el mandato **reset NAT**.
Exit	Hace volver al nivel de mandato anterior. Consulte “Salida de un entorno de nivel inferior” en la página xxv.

List

Utilice el mandato **list** para visualizar información sobre la configuración de NAT.

Sintaxis:

list
- all
- binding
- fragment
- global
- reserve
  - pools
  - addresses
- statistics
- translate

En el ejemplo siguiente, el tiempo se visualiza en horas, minutos y segundos. La antigüedad de la entrada es el tiempo que ha transcurrido desde que la estrada se utilizó por última vez. Enlace significa que se ha establecido una sección entre estas dos direcciones. Los tiempos de espera determinan el tiempo que transcurrirá después de la última comunicación hasta que se elimine un enlace. Consulte el mandato **set** de Talk 6 si desea obtener más información sobre los tiempos de espera.

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 enlaces, libera toda la memoria utilizada por NAT y reinicia NAT según la configuración actual de Talk 6. Cuando se reinicia NAT no se interrumpe ningún otro componente del 2212.

Sintaxis:

reset n**at**

Capítulo 28. Utilización de un servidor Acceso de marcación a las LAN (DIALs)

Un Servidor DIALs permite a los usuarios remotos establecer una conexión de entrada con una LAN y acceder a los recursos de la LAN del mismo modo que si estuvieran conectados localmente con un adaptador de LAN. De manera similar, el Servidor DIALs también permite a los usuarios conectados a la LAN establecer una conexión de salida con los recursos de la WAN (como, por ejemplo, boletines de anuncios, máquinas de FAX, Internet Service Providers (ISP) y otros servicios en línea), con lo cual desaparece la necesidad de una línea telefónica analógica y de módem en su estación de trabajo.

el Servidor DIALs se puede configurar simultáneamente tanto para usuarios de conexión de entrada como para usuarios de conexión de salida. El IBM DIALs Dial-In Client se ejecuta en la estación de trabajo remota y proporciona la función de establecimiento de conexión de entrada. La Figura 43 en la página 452 muestra un ejemplo de un dispositivo utilizado como un Servidor DIALs que ofrece soporte para la función de establecimiento de conexión de entrada.

Utilización de DIALs

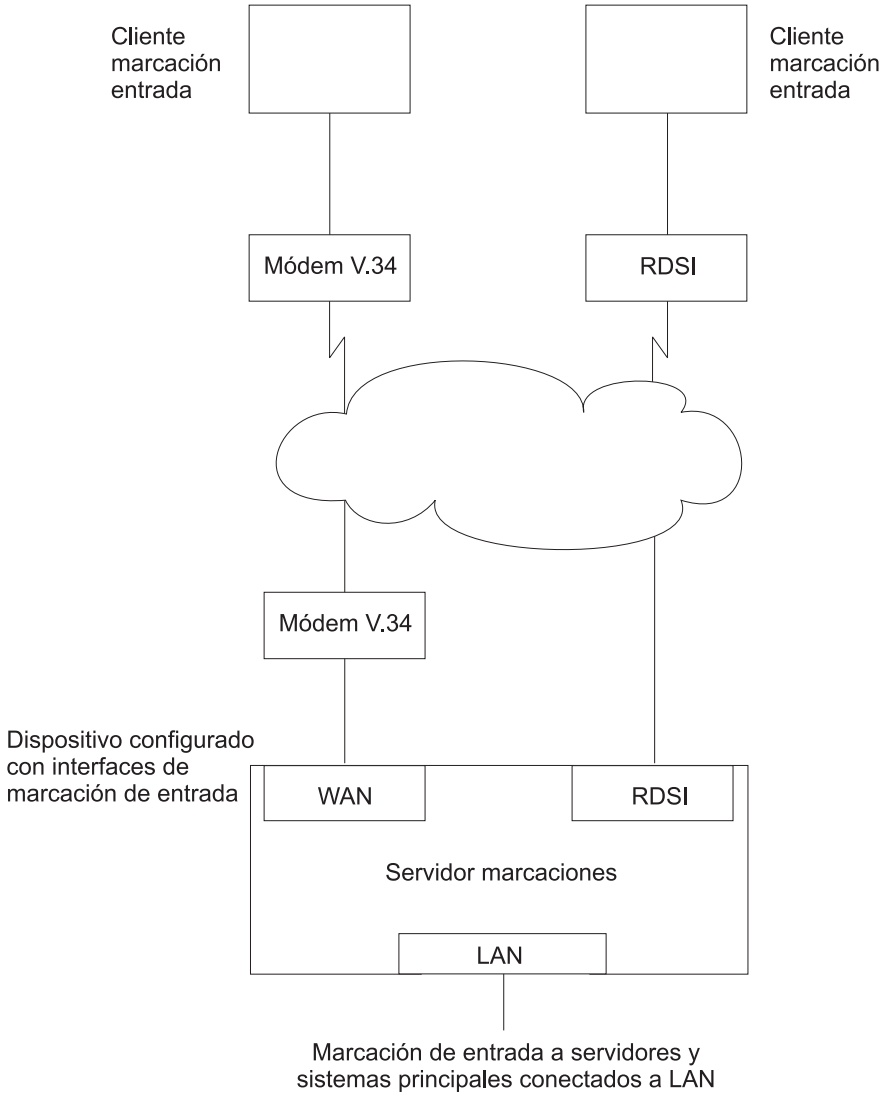


Figura 43. Un ejemplo de Servidor DIALs que ofrece soporte a establecimiento de conexión de entrada

El IBM DIALs Dial-Out Client se ejecuta en la estación de trabajo conectada a la red y proporciona la función de establecimiento de conexión de salida. Figura 44 en la página 453 muestra un ejemplo de un 2212 utilizado como un Servidor DIALs que ofrece soporte para la función de establecimiento de conexión de salida.

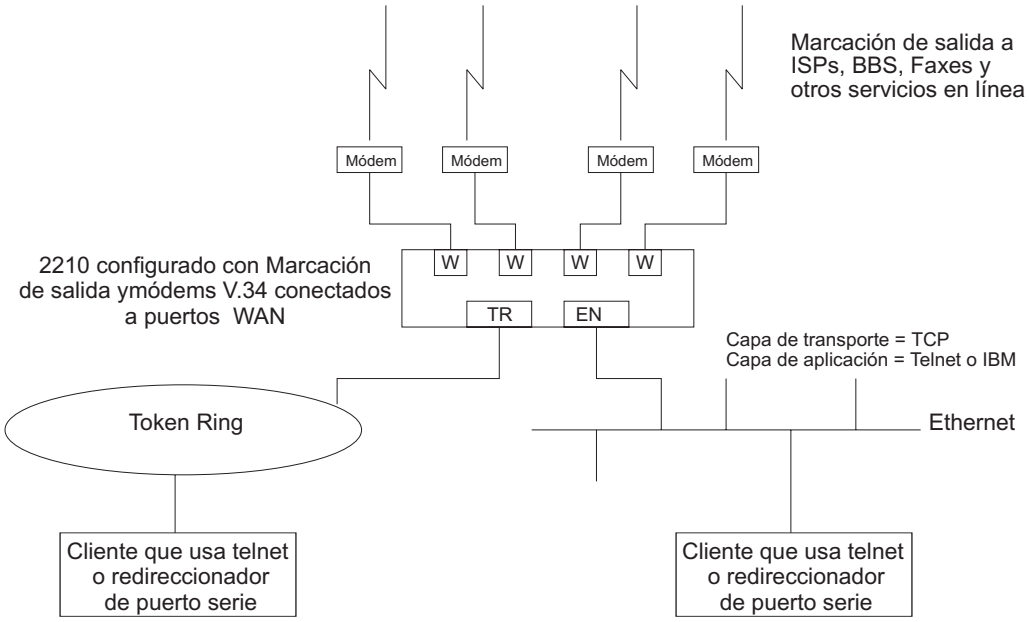


Figura 44. Un ejemplo de Servidor DIALs que ofrece soporte a establecimiento de conexión de salida,

Antes de la utilización de Dial-In-Access

Antes de utilizar Dial-In Access, es necesario que:

- Una estación de trabajo ejecute el IBM DIALs Dial-In Client u otro cliente de establecimiento de conexión de entrada PPP (a los que se hará referencia con los nombres ***cliente de establecimiento de conexión de entrada*** o ***cliente de establecimiento de conexión de entrada PPP*** a lo largo de las siguientes secciones).
- Existan configuraciones de protocolo completadas en la máquina cliente.
- Existan las interfaces RDSIy RDSI/Módem digital, las interfaces de módem integrado, una interfaz de módem nulo o módems V.34 externos conectados a puertos WAN del 2212 que desee utilizar para el establecimiento de una conexión de entrada de un único usuario.
- Que haya un Servidor DIALs totalmente configurado en la LAN.

Configuración de Dial-In Access

Esta sección describe cómo configurar tanto función de establecimiento de conexión de entrada como la de establecimiento de conexión de salida en el Servidor DIALs. La configuración de un cliente para utilizar Dial-In Access se describe en la documentación asociada con el cliente que la estación de trabajo utiliza.

Configuración de interfaces de establecimiento de conexión de entrada

Las interfaces de establecimiento de conexión de entrada del 2212 son un tipo especial de circuitos de establecimiento de conexión. Como la mayoría de los valores de un circuito de establecimiento de conexión habitual no son importantes

para las aplicaciones de establecimiento de conexión de entrada de un único usuario, se puede añadir un nuevo tipo de dispositivo denominado ***dial-in*** que establezca los valores por omisión adecuados para el circuito de establecimiento de conexión. Al añadir un dispositivo de establecimiento de conexión de entrada también se configuran los valores por omisión de configuración del encapsulador PPP que trabajan con la mayoría de clientes de establecimiento de conexión de entrada PPP, incluido el IBM DIALs Dial-In client. Estos valores por omisión se describen en "Valores por omisión de parámetros de circuitos de establecimiento de conexión para interfaces de establecimiento de conexión de entrada" y "Parámetros de encapsulador PPP de circuito de establecimiento de conexión para circuitos de establecimiento de conexión de entrada" en la página 455.

Nota: La función DIALs sólo se puede habilitar en circuitos de establecimiento de conexión de entrada. Los circuitos de establecimiento de conexión de entrada sólo reciben soporte en redes base V.34, RDSI y RDSI/Módem digital.

Valores por omisión de parámetros de circuitos de establecimiento de conexión para interfaces de establecimiento de conexión de entrada

Notas:

1. No altere temporalmente los parámetros descritos en esta sección. Si lo hace la función de establecimiento de conexión de entrada no funcionará correctamente.
2. Es probable que algunos parámetros no se visualicen o no se puedan configurar. Si desea obtener una descripción completa de los parámetros, consulte "Configuring and Monitoring Dial Circuits" en la publicación *Software de Access Integration Services Guía del usuario*.

Se establecen los siguientes valores por omisión cuando se añade una interfaz de establecimiento de conexión de entrada:

- El ***Tiempo de inactividad*** se establece en 0. Observe que se define un circuito estándar como circuito en los casos en que el temporizador de inactividad no tiene sentido. No será un circuito fijo con el que establecer una conexión de salida. La única vez que el circuito establecerá una conexión de salida será si se ha negociado una reclamación PPP o si se ha habilitado Multilink PPP en este circuito. Consulte "Shiva Password Authentication Protocol (SPAP)" y "Using the Multilink PPP Protocol" en la publicación *Software de Access Integration Services Guía del usuario* .
- Se permiten ***llamadas de entrada***. Se configuran todas las entradas porque los clientes de establecimiento de conexión de entrada no utilizan el intercambio LID implementado por los circuitos de establecimiento de conexión Nways.
- Se permiten ***llamadas de salida***.

  Nota: La "salida" para un circuito de establecimiento de conexión de entrada no es la misma que para un circuito de establecimiento de conexión de salida. Consulte "Antes de la configuración de interfaces de establecimiento de conexión de salida" en la página 456.

- Se configura una dirección de destino para "dirección_por_omisión". Esta dirección se añade a la lista de direcciones V.34. Como estas llamadas son de entrada y una reclamación o un intercambio Multilink PPP sólo dará como resultado llamadas de salida, la dirección de destino no tiene sentido. De todos

modos, la dirección es necesaria para los parámetros de circuito. No suprima esta dirección o sus circuitos se inhabilitarán.

Parámetros de encapsulador PPP de circuito de establecimiento de conexión para circuitos de establecimiento de conexión de entrada

Nota: Si desea obtener una descripción completa de los siguientes parámetros, consulte "Using Point-to-Point Protocol Interfaces" en la publicación *Software de Access Integration Services Guía del usuario.*

Se establecen los siguientes valores por omisión cuando se añade una interfaz de establecimiento de conexión de entrada:

- Se habilita la autenticación para SPAP, CHAP y PAP.
- El MRU de PPP se establece en 1522. Este tamaño de MRU es necesario para las versiones Windows 3.1, OS/2 y DOS del IBM DIALs Dial-In clients. No cambie este valor a menos que sepa que no está utilizando estos clientes.
- Habilita de manera automática DIALs en el encapsulador PPP. Ello activa algunas de las funciones importantes para los usuarios de Acceso de marcación a las LAN, como pueden ser el protocolo NetBIOS Control, el protocolo NetBIOS Frame Control, el tiempo restante, la autenticación SPAP, reclamaciones, identificación LCP y la adición y supresión automáticas de las rutas estáticas IP que van al cliente. Consulte "Using Point-to-Point Protocol Interfaces" en la publicación *Software de Access Integration Services Guía del usuario* si desea obtener más información sobre las funciones DIALs.

Adición de una interfaz de establecimiento de conexión de entrada

Para añadir una interfaz de establecimiento de conexión de entrada:

1. Configure una interfaz V.34, RDSI o RDSI/Módem digital en el 2212. Consulte "Using the V.34 Network Interface" en la publicación *Software de Access Integration Services Guía del usuario* si desea obtener detalles sobre la configuración. Consulte " Using the ISDN Interface" en la publicación *Software de Access Integration Services Guía del usuario* para obtener información sobre interfaces RDSI y de módem digital.
2. Entre **talk 6** para acceder al indicador `Config >`.
3. Entre **add device dial-in** en el indicador `Config >` para añadir la interfaz de establecimiento de conexión de entrada. Se le solicitará cuántos circuitos de establecimiento de conexión de entrada desea añadir. Este mandato creará las nuevas redes, informará sobre sus números de red, solicitará el número de red base y solicitará la habilitación de Multilink PPP.

   Ejemplo: Suponga que la red máxima actual es 3 y que desea agregar 1 red de establecimiento de conexión de entrada a la red base 2.

La Figura 45 es un ejemplo de definición de una interfaz de establecimiento de conexión de entrada.

Figura 45. Adición de una interfaz de establecimiento de conexión de entrada

```
Config>add dev dial-in
Adding device as interface 4
Defaulting Data-link protocol to PPP
Use "net 4" command to configure circuit parameters
Base net for this circuit [0]? 2

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               CSR  81600, CSR2  80C00, vector 94
Ifc 1     V.34 Base Net          CSR  81620, CSR2  80D00, vector 93
Ifc 2     V.34 Base Net          CSR  81640, CSR2  80E00, vector 92
Ifc 3     PPP Dial-in Circuit
Ifc 4     PPP Dial-in Circuit
```

Antes de la configuración de interfaces de establecimiento de conexión de salida

Antes de configurar y utilizar las interfaces de establecimiento de conexión de salida en el 2212, es necesario que:

- El software IBM con soporte para DIALs esté cargado en un 2212.
- Se disponga de un módem V.34 externo, un módem integrado o un módem nulo, si se conecta con un puerto de WAN disponible en el 2212. Consulte "Using the V.34 Network Interface" en la publicación *Software de Access Integration Services Guía del usuario* si desea obtener información de configuración.
- Se disponga de una estación de trabajo conectada a la LAN que tenga acceso al 2212 Servidor DIALs.
- Se disponga de software en el cliente como, por ejemplo, telnet, un direccionador de telnet o los IBM DIALs Dial-Out Clients. IP debe estar configurado correctamente en el cliente para que el cliente de establecimiento de conexión de salida funcione.

Utilización del módem nulo

Cuando utilice un módem nulo, utilice el reconocimiento completo D25NM-3:

Correlación de patillas:

1 con 1	**1 con 1**
2 con 3	**3 con 2**
4 con 5	**5 con 4**
6 con 8, 20	**8, 20 con 6**
7 con 7	**7 con 7**

Configuración de interfaces de establecimiento de conexión de salida

Los siguientes pasos describen la manera de configurar una interfaz de establecimiento de conexión de salida en el dispositivo.

1. Conecte un módem V.34 al puerto de WAN que utilizará como interfaz de establecimiento de conexión de salida.

2. Conecte con la consola del 2212 Servidor DIALs.
3. Entre **talk 6** en el indicador *.
4. Configure una interfaz V.34. Consulte " Using the V.34 Network Interface" en la publicación *Software de Access Integration Services Guía del usuario* si desea obtener más detalles.
5. Añada una interfaz de establecimiento de conexión de salida mediante el mandato **add device dial-out**. Cuando se le solicite la interfaz, utilice un número de interfaz V.34.

   Notas:

   a. Se pueden configurar varios circuitos en el principio de una red base V.34. De todos modos, sólo puede haber activo un circuito en un momento determinado.

   b. El software define una dirección V.34 denominada ***dirección_por_omisión***. No suprima esta dirección tal y como requiere el establecimiento de conexión de salida y éste no funcionará sin ella.
6. Configure el servidor de autenticación PPP, si está configurando el IBM DIALs Dial-Out Client y añada usuarios PPP, tal y como se describe en " PPP Authentication Protocols" en la publicación *Software de Access Integration Services Guía del usuario*. Los usuarios PPP añadidos deben tener el establecimiento de conexión de salida habilitado. El establecimiento de conexión de salida mediante telnet no requiere autenticación, por lo tanto no configure la autenticación para sesiones telnet.
7. Configure los parámetros de establecimiento de conexión de salida global mediante el mandato **feature dials**. Consulte el mandato **feature** en la publicación *Software de Access Integration Services Guía del usuario*.

   En este entorno puede configurar el temporizador de inactividad de establecimiento de conexión de salida, el nombre del servidor de establecimiento de conexión de salida, las agrupaciones de módems y otros parámetros.
8. Para que el IBM DIALs Dial-Out Client funcione correctamente, se debe definir una comunidad SNMP con acceso de lectura otorgado a todos los clientes de establecimiento de conexión de salida que deban poder utilizar el servidor de establecimiento de conexión de salida. Esto es obligatorio para que la aplicación de seleccionador de establecimiento de conexión de salida pueda descubrir los servidores de establecimiento de conexión de salida en la red. Consulte "SNMP Management" en la publicación *Configuración y supervisión de protocolos - Manual de consulta Volumen 1* si desea obtener información sobre el modo de configurar un comunidad SNMP.
9. Reinicie el dispositivo.

Configuración de agrupaciones de módems

Las agrupaciones de módems se definen como un grupo de módems que aparecen ante el usuario como un solo módem. Cuando el usuario necesita establecer una conexión de salida, se utilice el primer módem disponible de esta agrupación. Las agrupaciones de módems se crean en el 2212 Servidor DIALs definiendo grupos de interfaces de establecimiento de conexión de salida con el mismo nombre de puerto. Por omisión, todas las interfaces de establecimiento de conexión de salida se denominan "TODOS_PUERTOS", lo que crea una agrupación de módems. El asignar un nombre de manera individual a las interfaces de establecimiento de conexión de salida le permite a un usuario seleccionar un módem concreto para establecer una conexión de entrada.

Utilización de DIALs

Para configurar una agrupación de módems:

1. Entre **talk 6** en el indicador *.
2. Entre **net *n***, donde ***n*** es el número de la interfaz de establecimiento de conexión de salida, tal y como se define en “Using the V.34 Network Interface” en la publicación *Software de Access Integration Services Guía del usuario*. Esta acción le sitúa en el entorno de configuración de la interfaz.
3. Entre **encapsulator** (consulte “ Configuring and Monitoring Dial Circuits” en la publicación *Software de Access Integration Services Guía del usuario*) en el indicador `Circuit Config>`. Esta acción le sitúa en el entorno de configuración de establecimiento de conexión de salida.
4. Entre **set portname** en el indicador `Dial-out Config>`. Esta acción le solicitará el nombre del puerto (hasta 30 caracteres). Si especifica un número de puerto existente, el módem se añade a la agrupación con ese nombre.
5. Reinicie el 2212.

Antes de la configuración de los parámetros de DIALs globales

Esta sección describe los parámetros de Servidor DIALs globales.

Direcciones IP proporcionadas por el servidor

El direccionador puede estar configurado para proporcionar una dirección IP para que un cliente de establecimiento de conexión de entrada la utilice mientras dure su conexión. La dirección que el direccionador asigne al cliente se puede recuperar de 4 maneras diferentes, que se listan a continuación por orden de prioridad:

1. ID de usuario

   Se puede almacenar una dirección IP en el perfil de usuario PPP para cada cliente. Cuando un cliente se conecta y pide una dirección IP, el direccionador recupera la dirección configurada en ese perfil de usuario PPP del usuario. Ello le permite al usuario obtener siempre la misma dirección IP pero obliga a que haya 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

   Se puede almacenar una dirección IP en la configuración de interfaces de establecimiento de conexión de entrada. Cuando un cliente conecta y pide una dirección IP, el direccionador recupera la dirección de la interfaz a través de la cual se ha efectuado la conexión. Este método obliga a que haya una dirección IP exclusiva para cada interfaz de establecimiento de conexión de entrada.

   Para establecer la dirección IP de la 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 de la interfaz.
   - Utilice el mandato `PPP Config>` **set ipcp** para establecer la dirección IP de interfaces.

3. Agrupación

   Se pueden almacenar bloques de direcciones IP en una agrupación de direcciones IP. Cuando un cliente se conecta y pide una dirección, el

direccionador recupera una dirección de la agrupación. Cuando el cliente se desconecta, la dirección vuelve a la agrupación. Este método proporciona una única ubicación para configurar direcciones IP del cliente de establecimiento de conexión de entrada sin la necesidad de un servidor de direcciones.

Utilice el mandato `DIALs config>` **add ip-pool** para añadir una agrupación de direcciones IP.

4. Proxy DHCP

   Se puede ceder una dirección IP de un servidor servidor DHCP. Cuando un cliente se conecta y pide una dirección, el direccionador solicita una dirección del servidor DHCP en nombre del cliente. Este método obliga a que un servidor DHCP esté presente en la LAN o configurado en el direccionador. Un servidor DHCP puede proporcionar direcciones para clientes en varios direccionadores. Consulte "Protocolo de configuración dinámica de sistemas principales (DHCP)" si desea obtener más información.

   Utilice el mandato `DIALs config>` **add dhcp-server** para agregar un servidor DHCP.

Métodos de asignación de direcciones IP

La dirección IP que un cliente de establecimiento de conexión de entrada utiliza durante la conexión puede proceder de cinco fuentes diferentes, que se listan en orden de preferencia:

1. cliente proporcionado
2. id de usuario asignado
3. interfaz asignada
4. agrupación de direcciones
5. servidor DHCP

Cuando un cliente de establecimiento de conexión de entrada se conecta, el direccionador va pasando por estas fuentes hasta que encuentra una dirección o agota todas las fuentes. Si no se puede encontrar ninguna dirección, la negociación IPCP falla. Se puede utilizar cualquier combinación de métodos.

La configuración por omisión es:

```
Client     :  Enabled
UserID     :  Enabled
Interface  :  Enabled
Pool       :  Enabled
DHCP Proxy :  Disabled
```

Nota: Por omisión, no hay direcciones configuradas en el perfil de usuario PPP, en la interfaz o en la agrupación de direcciones.

Protocolo de configuración dinámica de sistemas principales (DHCP)

El protocolo de configuración dinámica de sistemas principales (DHCP) se ha desarrollado para proporcionar parámetros de configuración a sistemas principales de una red. Entre otros parámetros de configuración, DHCP dispone de un mecanismo para la asignación de direcciones de red a sistemas principales.

La función Proxy DHCP actúa como un cliente *en nombre* de un usuario PPP de establecimiento de conexión de entrada. Ello permite al dispositivo obtener una

cesión de dirección IP durante la sesión de establecimiento de conexión de entrada o hasta que la cesión finalice. La dirección IP que se ha asignado desde el servidor DHCP se comunica con el cliente de establecimiento de conexión de entrada mediante PPP IPCP (consulte "IP Control Protocol" en la publicación *Software de Access Integration Services Guía del usuario* si desea obtener una descripción de IPCP). El software del cliente de establecimiento de conexión de entrada no tiene conocimiento de que DHCP se haya utilizado para asignar una dirección IP y, por lo tanto, no requiere activación de DHCP alguna.

Proxy DHCP obliga a que por lo menos un servidor DHCP esté configurado y sea accesible desde el direccionador.

Proxy DHCP obliga a que las direcciones que se están asignando a usuarios de establecimiento de conexión de entrada estén dentro de la misma subred de una LAN conectada directamente. En una configuración habitual, ello obliga a que se habilite el direccionamiento de subred de proxy ARP a fin de que el direccionador pueda responder las peticiones ARP de sistemas principales de la red local en nombre de los clientes de establecimiento de conexión de entrada.

Configuración DHCP básica

La configuración más básica llama a un único servidor DHCP de la misma red que el direccionador, con las direcciones de establecimiento de conexión de entrada a ceder dentro de la misma subred que esta LAN.

Cuando el cliente establece una conexión de entrada, se obtiene la cesión de una dirección IP del servidor DHCP que se utiliza en la negociación IPCP con el cliente.

1. Conecte el 2212 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 ceder direcciones IP. Recuerde que las direcciones IP a ceder DEBEN estar dentro de una subred de una LAN conectada de manera directa y proxy ARP debe estar habilitado en el 2212).
3. La configuración habitual de 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 un servidor DHCP (`Dials Config>` **add dhcp 10.0.0.111**)
5. Establezca el software de cliente de establecimiento de conexión de entrada en *Servidor asignado.*

   Notas:

   a. La configuración de *Servidor asignado* varía entre las diferentes implementaciones de clientes de establecimiento de conexión de entrada.

   b. El software de cliente no debe estar configurado para obtener su dirección de DHCP. El cliente debe obtener su dirección enviando una dirección de 0.0.0.0 a IPCP en la petición de configuración inicial.

6. Para esta configuración, deje el valor por omisión de DHCP GATEWAY ADDRESS en 0.0.0.0.

Varios saltos para acceder al servidor DHCP

Los servidores configurados DHCP deben ser direcciones IP a las que se pueda acceder desde el direccionador conectado. Es necesario que se pueda aplicar siempre ping al servidor desde el recuadro de acceso remoto.

Cuando el servidor DHCP se encuentra a una distancia de varios saltos, es necesario que el servidor conozca una dirección a la cual responder y que indique la agrupación desde la que se debe asignar una dirección IP. La agrupación desde la que se debe asignar una IP es importante porque el servidor DHCP se puede utilizar para servir direcciones a un número determinado de subredes y debe haber, así mismo, alguna indicación en cuanto a la agrupación de direcciones desde donde se debe hacer la selección. La dirección de pasarela DHCP (*giaddr*) se utiliza para esto (esta terminología se base en la definición que establece RFC 2131). La *giaddr* debe ser una dirección que sea local para el 2212, como la red en anillo el puerto LAN de Ethernet. Además, como *giaddr* es la dirección que el servidor DHCP utilizará para responder, asegúrese de que puede aplicar ping a esta dirección desde el mismo servidor DHCP.

Red de varios servidores DHCP

Puede configurar varios servidores DHCP para obtener redundancia. Cuando se configuran varios servidores, el cliente Proxy DHCP solicita a todos los servidores una dirección y acepta la primera respuesta que recibe. Si alguno de los servidores DHCP están a más de un salto de distancia o están conectados a una subred que no está asociada con las direcciones de esta agrupación, se debe configurar la *giaddr*. Consulte “Varios saltos para acceder al servidor DHCP”.

Aunque puede haber más de un servidor DHCP que ofrezca direcciones, es importante no dejar que la agrupación de direcciones configurada de cada servidor se solape. Así mismo, como sólo hay una *giaddr* a la que el servidor DHCP deba responder y con la que éste deba llevar a cabo una búsqueda, cada agrupación de direcciones debe hallarse en la misma subred que la otra.

Servidor de nombres de dominio dinámico (DDNS)

Un servidor de nombres de dominio (DNS) correlaciona direcciones IP con nombres de sistema principal y habitualmente es estático por naturaleza. El DNS dinámico es una función que, cuando se utiliza con el servidor DDNS DHCP y un servidor DNS, permite que DHCP actualice de manera dinámica el servidor DNS con una dirección IP y una correlación de nombres de sistema principal. Dicha función sólo se puede utilizar junto con el Proxy DHCP.

Cuando se habilita un DNS dinámico en el 2212 y se configura un nombre de sistema principal en el perfil de usuario (consulte “PPP Authentication Protocols” en la publicación *Software de Access Integration Services Guía del usuario*), ese nombre de sistema principal pasa como opción 81 (DDNS) al servidor DHCP. Si ha configurado el servidor DHCP correctamente para DDNS, el servidor DHCP actualiza el servidor DDNS con la dirección IP que se ha cedido al direccionador y el nombre del sistema principal que el direccionador le ha enviado. Ello permite a los demás usuarios acceder al cliente de establecimiento de conexión de entrada a través del nombre del sistema principal evitando la necesidad de que el cliente conozca la dirección IP seleccionada de manera dinámica.

Capítulo 29. Configuración de DIALs

Este capítulo describe la configuración de DIALs y sus mandatos operativos. Consta de las siguientes secciones:

- "Acceso al entorno de configuración global de DIALs"
- "Mandatos de configuración global de DIALs"
- "Acceso al entorno de supervisión global de DIALs" en la página 472
- "Mandatos de supervisión global de DIALs" en la página 472
- "Supervisión de interfaces de establecimiento de conexión de entrada" en la página 476
- "Supervisión de interfaces de establecimiento de conexión de salida" en la página 476

Acceso al entorno de configuración global de DIALs

Utilice el procedimiento siguiente para acceder al proceso de configuración global.

1. En el indicador OPCON, entre **talk 6**. (Si desea obtener más información sobre este mandato, consulte *The OPCON Process and Commands* en la publicación Software de Access Integration Services Guía del usuario). Por ejemplo:

   ```
   * talk 6
   Config>
   ```

   Después de entrar el mandato **talk 6**, el mandato CONFIG (`Config>`) aparece en el terminal. Si el indicador no aparece cuando se entra por primera vez la configuración, pulse **Intro** de nuevo.
2. Entre el mandato **feature dials** en el indicador CONFIG para acceder al indicador `DIALs Config>` y al entorno de configuración de parámetros globales de DIALs.

Mandatos de configuración global de DIALs

Tabla 54 (Página 1 de 2). Mandatos de configuración global de DIALs

Mandato	Función
? (Ayuda)	Visualiza todos los mandatos disponibles para este nivel de mandato, o lista las opciones de mandatos específicos (si es que están disponibles). Consulte "Obtención de ayuda" en la página xxv.
Add	Añade un servidor DHCP (protocolo de configuración dinámica de sistemas principales) 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 métodos de asignación de direcciones IP, protocolos de establecimiento de conexión de salida, MP multichasis, SPAP Banner y DNS dinámico.
Enable	Habilita varios métodos de asignaciones de direcciones IP, protocolos de establecimiento de conexión de salida MP multichasis, SPAP Banner y DNS dinámico.
List	Lista los parámetros globales de DIALs y sus valores.

Tabla 54 (Página 2 de 2). Mandatos de configuración global de DIALs

Mandato	Función
Set	Establece el tiempo permitido, la dirección de la pasarela dhcp, las direcciones del servidor de nombres NetBIOS, las direcciones MAC asignadas localmente, las conexiones virtuales (VC) las direcciones del servidor de nombres dinámico, el temporizador de inactividad del establecimiento de conexión de salida y el nombre del servidor de establecimiento de conexión de salida.
Exit	Hace volver al nivel de mandato anterior. Consulte “Salida de un entorno de nivel inferior” en la página xxv.

Add

Utilice el mandato **add** para añadir un nuevo servidor Proxy DHCP a un 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 ceden, por su parte, las direcciones a clientes de establecimiento de conexión de entrada. Se pueden añadir varios servidores para obtener redundancia. El número máximo de servidores es 20.

La agrupación de direcciones IP proporciona un método mediante el cual el direccionador puede recuperar una dirección IP de una agrupación de direcciones definida localmente para un cliente de establecimiento de conexión de entrada. El cliente puede utilizar dicha dirección durante toda la conexión con el direccionador. Una agrupación consta de uno o más bloques de direcciones IP. El número máximo de bloques es 20. Cada uno de dichos bloques se define mediante una dirección IP base y el número de direcciones del bloque. Las direcciones de cada bloque son ascendentes y contiguas, empezando por la dirección base.

Sintaxis:

a**dd** dhcp-server *dirección_ip*
ip-pool *dirección_base n_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 n_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 Proxy DHCP de la lista de servidores o para eliminar un bloque de direcciones de la agrupación de direcciones IP.

Sintaxis:

de**lete** dhcp-server *dirección_ip*

ip-pool *dirección_base n_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 n_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, protocolos de establecimiento de conexión de salida, SPAP Banner y DNS dinámico.

Sintaxis:

di**sable** dynamic-dns

dial-out

ip-address-assignment *tipo*

spap-banner

dial-out ***tipo***
Inhabilita el uso del establecimiento de conexión de salida con telnet o clientes IBM DIALs Dial-Out. Puede especificar:

dials Inhabilita todos los clientes IBM DIALs

telnet Inhabilita todos los clientes telnet.

Para inhabilitar ambos tipos de clientes, debe entrar el mandato disable dial-out para cada uno de los tipos. Si se inhabilitan ambos tipos de clientes, se inhabilita el establecimiento de conexión de salida en el 2212.

dynamic-dns
Inhabilita el envío de DHCP opción 81 para el nombre de sistema principal del usuario. Consulte “Servidor de nombres de dominio dinámico (DDNS)” en la página 461 si desea obtener más información.

IP-address-assignment ***tipo***
Inhabilita varias técnicas de asignación de direcciones IPCP. Puede especificar una de las 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 IPCP para la interfaz.
- Agrupación – Evita que el direccionador utilice la agrupación de direcciones IP para asignar direcciones a clientes.
- Proxy DHCP – Evita que el direccionador ceda una dirección del servidor DHCP.

Consulte “Direcciones IP proporcionadas por el servidor” en la página 458 si desea obtener información adicional sobre las técnicas de asignación.

spap-banner
Inhabilita el envío de un banner SPAP a un usuario remoto autenticado con SPAP.

Nota: Si se entra \n se forzará un carácter de nueva línea en el banner que se visualiza en el cliente.

Enable

Utilice el mandato **enable** para habilitar la asignación de direcciones IP, protocolos de establecimiento de conexión de salida SPAP Banner y DNS dinámico.

Sintaxis:

enable dynamic-dns
ip-address-assignment . . .
spap-banner

dial-out *tipo*
Habilita el uso del establecimiento de conexión de salida con telnet o clientes IBM DIALs Dial-Out. Ambos tipos de clientes están habilitados por omisión. Puede especificar:

dials Habilita todos los clientes IBM DIALs

telnet Habilita todos los clientes telnet.

dynamic-dns
Inhabilita el envío de DHCP opción 81 para el nombre de sistema principal del usuario. Consulte “Servidor de nombres de dominio dinámico (DDNS)” en la página 461 si desea obtener más información.

IP-address-assignment *tipo*
Habilita varias técnicas de asignación de direcciones IPCP. El direccionador probará todos los métodos habilitados en el orden que se lista. Puede especificar uno de las 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 no es cero, será ofrecida al cliente.
- Interfaz – El direccionador buscará en la dirección IP configurada en la interfaz. Si la dirección no es cero, será ofrecida al cliente.
- Agrupación – El direccionador solicitará una dirección de la agrupación de direcciones IP. Si hay una dirección disponible, será ofrecida al cliente.
- Proxy DHCP – El direccionador intentará ceder una dirección del DHCP. Si lo consigue, la dirección se le ofrecerá al cliente.

Consulte “Direcciones IP proporcionadas por el servidor” en la página 458 si desea obtener información adicional sobre las técnicas de asignación.

spap-banner

Habilita el envío de un banner SPAP a un usuario remoto autenticado con SPAP. Utilice el mandato **set spap-banner** que se describe en el mandato “Set” en la página 469 para entrar el texto del banner SPAP. Consulte “Shiva Password Authentication Protocol (SPAP)” en la publicación *Software de Access Integration Services Guía del usuario* si desea obtener más información.

List

Utilice el mandato **list** para visualizar la configuración actual. Los tiempos del estado DHCP y de cesión de cada red se pueden supervisar desde la consola punto a punto. Consulte el mandato **listipcp** en la publicación *Software de Access Integration Services Guía del usuario* si desea obtener un ejemplo.

Sintaxis:

list	all
	dhcp-servers
	dial out
	dynamic-dns
	ip-address-assignment
	ip-pools
	name-servers
	spap-banner
	time-allowed
	vc-parameters

Ejemplo:

Configuración de DIALs

```
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...

Box-level dial-out settings
Inactive timer:                                      15
LAN Protocols enabled for dial-out:         TELNET DIALs
Server name:                                          DIALOUT_SERVER

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 o no habilitadas. Recibiría esta sección de la pantalla y la sección que contiene los valores de establecimiento de conexión de salida de nivel de recuadro como respuesta al mandato **list ip-address-assignment**.

IP address pools
: Visualiza las agrupaciones de direcciones IP configuradas. Recibiría esta sección de la pantalla 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. Recibiría esta sección de la pantalla como respuesta al mandato **list dhcp-servers**.

Dynamic Name Servers
: Visualiza si el DNS dinámico está habilitado. Recibiría una sección de esta pantalla como respuesta al mandato **list dynamic-dns**.

primary domain server (dns)
Esta línea y las siguientes visualizan los servidores de nombres primario y secundario configurados. Recibiría esta sección de la pantalla como respuesta al mandato **list name-servers**.

time allowed
Visualiza el el tiempo máximo (en minutos) para los usuarios de dials. Recibiría esta sección de la pantalla como respuesta al mandato **list time-allowed**.

spap banner
Visualiza el contenido del banner spap. Recibiría esta sección de la pantalla como respuesta al mandato **list spap-banner**.

vc connections
Visualiza información sobre las conexiones virtuales configuradas.

multi-chassis mp
Visualiza el discriminador de puntos finales configurado.

Set

Utilice el mandato **set** para establecer el tiempo permitido, la dirección de pasarela, las direcciones del servidor de nombres de NetBIOS, las direcciones del servidor de nombres dinámico, el temporizador de inactividad del establecimiento de conexión de salida y el nombre del servidor de establecimiento de conexión de salida..

Sintaxis:

set dhcp-gateway-address
dial-out . . .
dns . . .
laa
multi-chassis-mp
nbns . . .
spap-banner . . .
time-allowed
vc-parameters

dhcp-gateway-address ***n_interfaz dirección_ip***
Establece la dirección IP asociada con la pasarela DHCP. DHCP utiliza la dirección como:

1. Una dirección a la que responde DHCP
2. Una indicación de la agrupación de direcciones desde la que DHCP asigna una dirección IP

Si el servidor DHCP no se halla en una interfaz LAN conectada de manera directa, deberá configurar entonces esta dirección como la dirección de una las interfaces LAN que dispone de conectividad IP con el servidor DHCP. Consulte “Protocolo de configuración dinámica de sistemas principales (DHCP)” en la página 459 y la definición de “giaddr” en RFC 1541 si desea obtener más información.

dial-out ***parámetro***
Establece el temporizador de inactividad o el nombre del servidor para redes de establecimiento de conexión de salida. El ***Parámetro*** puede ser:

inactivity-timer
Establece el temporizador de inactividad de establecimiento de conexión de salida para redes de establecimiento de conexión de salida. Se define como el tiempo, en minutos, durante el que un usuario puede estar conectado sin tráfico de datos en la conexión. Por ejemplo, si el temporizador de inactividad se establece en 5 minutos y durante un intervalo cualquiera de 5 minutos no se reciben ni transmiten datos, la conexión quedará desactivada y el módem estará disponible. El valor por omisión es 0, que significa que el temporizador de inactividad está inhabilitado y que se mantendrá la conexión de manera indefinida.

servername
Establece el nombre del servidor de establecimiento de conexión de salida. Puede ser cualquier cadena de hasta 30 caracteres. Por omisión es "2210_DIALS_SERVER". Se trata del nombre que los clientes IBM DIALs Dial-Out ven cuando utilizan la aplicación "Chooser" para descubrir servidores de establecimiento de conexión de salida. Este parámetro no tiene sentido para los clientes de establecimiento de conexión de salida de telnet.

dns ***tipo dirección_ip***
Configura los servidores de nombres de dominio primario y secundario (DNS). El ***Tipo*** puede ser:

primary
Establece la dirección IP del servidor DNS primario para que el cliente de establecimiento de conexión de entrada lo utilice. Este valor se negocia durante IPCP para algunos clientes de marcación (en concreto Windows 95).

secondary
Establece la dirección IP del servidor DNS secundario para que el cliente de establecimiento de conexión de entrada lo utilice. Este valor se negocia durante IPCP para algunos clientes de marcación (en concreto Windows 95).

laa *n_direcciones_MAC dirección_base_MAC*
Establece el número de direcciones MAC y la dirección base para la tabla de direcciones administradas localmente (LAA). Sólo utilizarán LAA las redes de túnel de capa 2.

n_direcciones_MAC
Especifica el número de direcciones Mac a añadir a la tabla LAA, empezando por la *Dirección_Base_MAC*.

Valores válidos: de 0 a 256

Valor por omisión: 0

base_direcciones_MAC
Especifica la dirección MAC base de la tabla 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]? 002210aaaaaa
    DIALs Config>
```

multi-chassis-mp

Establece el discriminador de punto final a utilizar. Todos los enlaces que deben unir el mismo paquete deben disponer del mismo discriminador de punto final.

Ejemplo:

```
DIALs Config> set multi-chassis-mp
   Enter Endpoint Discriminator to use from stacked group (0 for box S/N): 2345
```

nbns ***tipo adreça_ip***

Configura los servidores NetBIOS de nombres primario y secundario. El ***Tipo*** puede ser:

primary

Establece la dirección IP del servidor de nombres NetBIOS primario.

secondary

Establece 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 han completado de manera satisfactoria la autenticación SPAP.

Ejemplo:

```
DIALs config>set spap-banner
SPAP banner  :Disabled

Enter Banner: Welcome to the network...
```

time-allowed

Establece el tiempo permitido para los usuarios de establecimiento de conexión de entrada PPP y los usuarios de establecimiento de conexión de salida.. Este parámetro define el tiempo máximo (en minutos) que un usuario puede estar conectado. El valor por omisión es 0, lo que significa que el usuario se puede conectar durante tiempo ilimitado.

vc-parameters

Utilice este parámetro para establecer los atributos de conexión virtual por omisión. El sistema le solicita el número máximo de conexiones, el tiempo máximo de suspensión y el valor del 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

El número máximo de conexiones virtuales que pueden estar activas o suspendidas. Cuando utilice VC con MP, configure este valor para que sea un número más que el número de conexiones físicas.

Valores válidos: de 0 a 255

Valor por omisión: 50

Maximum suspended time
El tiempo máximo, en horas, que una conexión virtual puede estar suspendida antes de que el sistema finalice la conexión. Si se especifica 0 para este parámetro, se permite que una conexión virtual esté suspendida de manera indefinida.

Valores válidos: de 0 a 48

Valor por omisión: 12

Inactivity Timeout
El número de segundos que una conexión virtual puede estar inactiva antes de que se suspenda.

Valores válidos: de 10 a 1024

Valor por omisión: 30

Acceso al entorno de supervisión global de DIALs

Utilice el siguiente procedimiento para acceder a los mandatos de supervisión de DIALs.

1. Entre **talk 5** en el indicador OPCON. (Si desea obtener detalles sobre este mandato, consulte el capítulo "The OPCON Process and Commands" en la publicación *Software de Access Integration Services Guía del usuario*.) Por ejemplo:

   ```
   * talk 5
   +
   ```

   Después de entrar el mandato **talk 5**, el indicador GWCON (+) aparece en el terminal. Si el indicador no aparece cuando se entra por primera vez la configuración, pulse **Intro** de nuevo.
2. Entre el mandato **feature dials** en el indicador + para acceder al indicador `DIALS Console>` y al entorno de supervisión global.

   Ejemplo:

   ```
   + feature dials
   DIALS Console>
   ```

Mandatos de supervisión global de DIALs

Tabla 55. Mandatos de supervisión global DIALs

Mandato	Función
Clear	Borra una conexión virtual suspendida específica.
List	Visualiza el estado de varias conexiones virtuales o de todas las conexiones virtuales.
Reset	Activa de manera dinámica los parámetros de DIALS.
Exit	Hace volver al nivel de mandato anterior. Consulte "Salida de un entorno de nivel inferior" en la página xxv.

Clear

Utilice el mandato **clear** para borrar conexiones virtuales suspendidas específicas.

Sintaxis:

clear vc *id_conexión*

vc *id_conexión*

Especifica la conexión virtual suspendida que está finalizando. Para obtener el *id_conexión*, entre el mandato **list all-vc** o el mandato **list suspended-vcs**.

List

Utilice el mandato **list** para visualizar todas las conexiones virtuales, las conexiones virtuales activas, las conexiones virtuales suspendidas o los valores de los parámetros vc.

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. Consulte la descripción del parámetro **all-vcs** si desea obtener una descripción 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:

Configuración de DIALs

```
+ 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
========== ========= ============ HHH:MM:SS ================
1656494850         8           30   0:26:15 don
7293521502         9           30   1:41:57 jane


Suspended VCs:
           Hrs.Max
Conn ID    Suspend Suspended Username
========== =======  HH:MM:SS ======================
9256166098      12   0: 4:13 joe
```

Los atributos de las VC activas y suspendidas son:

Conn ID
El id de conexión de la conexión virtual. El sistema asigna el id cuando establece la conexión.

Username
El AAA. El usuario RADIUS o de la lista local que establece la conexión virtual.

Para VC activas:

Interface
La interfaz de red que gestiona la conexión virtual.

Nota: No asigne direcciones IP a clientes de marcación mediante la asignación de interfaces para evitar problemas generados por otros usuarios que utilizan la interfaz que la VC ha suspendido.

Idle Timeout
El tiempo de inactividad, en segundos, al cabo del cual el sistema suspenderá la VC. Corresponde al valor del temporizador de inactividad del mandato **set**.

Connected HHH:MM:SS
El tiempo total en horas, minutos y segundos que la VC ha estado conectada a una interfaz.

Para VC suspendidas:

Hrs. Max Suspended
El número máximo de horas que una VC puede estar en estado de suspensión antes de que el sistema finalice la conexión.

Corresponde al valor del tiempo de suspensión máximo del mandato **set**.

Suspended HH:MM:SS
El tiempo total en horas, minutos y segundos que la VC ha estado suspendida.

dhcp-servers
Visualiza información configurada sobre servidores DHCP y sus direcciones IP.

ip-address-assignment
Visualiza los métodos mediante los cuales las direcciones IP se pueden asignar 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

Note: The * indicates from which block the next address will be retrieved.
```

suspended-vcs
Visualiza los atributos de todas las conexiones virtuales suspendidas. Consulte la descripción del parámetro **all-vcs** si desea obtener una descripción de los atributos.

vc-parameters
Visualiza los valores de los parámetros vc que se han establecido mediante el mandato **set vc-parameters**.

Reset

Utilice el mandato **reset** para activar de manera dinámica los cambios de configuración efectuados a la interfaz de DIALs en `talk 6`.

Sintaxis:

reset all

dhcp-parameters

ip-address-assignment

ip-pool

vc-parameters

all Activa de manera dinámica el DHCP, la asignación de direcciones IP y los cambios de configuración de agrupaciones IP.

dhcp-parameters
Activa de manera dinámica la configuración DHCP.

ip-address-assignment
Activa de manera dinámica la configuración de métodos de asignación de direcciones IP.

ip-pool
Activa de manera dinámica la configuración de agrupaciones de direcciones IP.

vc-parameters
Actualiza de manera dinámica los cambios de configuración de VC.

Mandatos de configuración de la interfaz de establecimiento de conexión de salida

Para acceder al entorno de los parámetros de la interfaz de establecimiento de conexión de salida:

1. Entre **talk 6** en el indicador `*`.
2. Entre **net *n*** en el indicador `Config >`.
3. Entre **encapsulator** en el indicador `Circuit config: n>`.

La Tabla 56 lista los mandatos disponibles desde el indicador `dial-out config>`.

Tabla 56. Mandatos de configuración de la interfaz de establecimiento de conexión de salida

Mandato	Función
? (Ayuda)	Visualiza todos los mandatos disponibles para este nivel de mandato, o lista las opciones de mandatos específicos (si es que están disponibles). Consulte "Obtención de ayuda" en la página xxv.
Set	Define el nombre de puerto asociado con un módem.
Exit	Hace volver al nivel de mandato anterior. Consulte "Salida de un entorno de nivel inferior" en la página xxv.

Set

Utilice el mandato **set** para definir el nombre de puerto de un módem.

Sintaxis:

set portname *nombre*

portname
Define el nombre del puerto asociado con un módem. Utilice este nombre para definir ***agrupaciones de módem.*** El nombre puede tener hasta 30 caracteres.

Valor por omisión: ALL_PORTS

Ejemplo: `dial-out config>`**set portname localcalls**

Supervisión de interfaces de establecimiento de conexión de entrada

La supervisión de interfaces de establecimiento de conexión de entrada es la misma que para la supervisión de otros circuitos de establecimiento de conexión PPP. Si desea obtener más detalles, consulte "Configuring and Monitoring Point-to-Point Protocol Interfaces" en la publicación *Software de Access Integration Services Guía del usuario.*

Supervisión de interfaces de establecimiento de conexión de salida

La Tabla 57 en la página 477 lista los mandatos disponibles para la supervisión de interfaces de establecimiento de conexión de salida.

Tabla 57. Mandatos de configuración de interfaces de establecimiento de conexión de salida

Mandato	Función
? (Ayuda)	Visualiza todos los mandatos disponibles para este nivel de mandato, o lista las opciones de mandatos específicos (si es que están disponibles). Consulte “Obtención de ayuda” en la página xxv.
Clear	Restablece las estadísticas de la interfaz de establecimiento de conexión de salida.
List	Lista el estado actual de la interfaz de establecimiento de conexión de salida, el número de bytes transmitidos y recibidos en esta interfaz y los parámetros actuales del cliente.
Exit	Hace volver al nivel de mandato anterior. Consulte “Salida de un entorno de nivel inferior” en la página xxv.

Clear

Utilice el mandato **clear** para restablecer las estadísticas del número de octetos recibidos y transmitidos por esta interfaz.

Sintaxis:

clear

Ejemplo:

```
clear
Statistics reset.
```

List

Utilice el mandato **list** para visualizar el estado actual de la interfaz de establecimiento de conexión de salida. El mandato **list** visualiza siempre el estado actual de la red de establecimiento de conexión de salida, el tiempo transcurrido desde el cambio de estado y el número de bytes recibidos y transmitidos.

Sintaxis:

list

Ejemplo de interfaz inactiva:

```
list
Dial-out Settings for current session:

Dial-out state is DOWN
Time since change           = 52 minutes and 34 seconds

Dial-out Octets transmitted = 0
Dial-out Octets received    = 0

Session down, no valid settings
```

Nota: Cuando un cliente se conecta a un puerto de establecimiento de conexión de salida mediante telnet, no hay presente ningún nombre de usuario porque el servidor no ha llevado a cabo ninguna autenticación.

Ejemplo de interfaz activa:

Configuración de DIALs

```
list
Dial-out Settings for current session:

Dial-out state is UP
Time since change           = 3 seconds

Dial-out Octets transmitted = 14
Dial-out Octets received    = 765

Current user                = not available
Time allowed for user       = unlimited
Inactivity timer for port   = 10 minutes
Line speed                  = 57600
Current DTR state           = DTR ON
Current dial-out protocol   = TELNET
Options negotiated:
        Will Suppress Go Ahead
        Wont' Echo characters
```

Ejemplo de cliente IBM DIALs Dial-Out:

```
list
Dial-out Settings for current session:

Dial-out state is UP
Time since change           = 12 seconds

Dial-out Octets transmitted = 11
Dial-out Octets received    = 756

Current user                = ebooth
Time allowed for user       = unlimited
Inactivity timer for port   = 10 minutes
Line speed                  = 57600
Current DTR state           = DTR ON
Current dial-out protocol   = DIALs
```

Capítulo 30. Utilización del Servidor DHCP

En este capítulo se describe el modo de utilización del Servidor DHCP. Consta de las secciones siguientes:

- "Introducción a DHCP"
- "Conceptos y terminología" en la página 484
- "Parámetros de servidor DHCP y de cesión" en la página 487
- "Opciones DHCP" en la página 487
- "Configuración de IP para DHCP" en la página 500
- "Configuración de ejemplo del servidor DHCP" en la página 501

Introducción a DHCP

El protocolo de configuración dinámicas de sistemas principales (DHCP) es un protocolo cliente/servidor basado en el protocolo de arranque (BOOTP). El servidor DHCP proporciona direcciones IP reutilizables controladas centralmente y otro tipo de información TCP/IP para clientes DHCP. Su funcionalidad puede mitigar el límite que se plantea a los gestores de red en cuanto a la distribución de información de configuración a usuarios nuevos y existentes. Esta función cumple con RFC 2131 pero ofrece soporte a muchas funciones adicionales que no se incluyen en dicho documento. Existe también soporte para clientes BOOTP tal y como se define en RFC 951.

Con el DHCP, los clientes con soporte pueden enviar mensajes de DESCUBRIMIENTO de difusión para encontrar servidores DHCP en su red y, en consecuencia, se les pueden OFRECER los datos de configuración de éstos de manera dinámica en la red. DHCP utiliza los puertos BOOTP UDP conocidos públicamente (68 para el servidor y 67 para el cliente) a fin de comunicar peticiones y respuestas. Los clientes y servidores DHCP pueden utilizar los agentes BOOTP Relay para ampliar el alcance de su servicio. DHCP ofrece muchas ventajas en redes configuradas de manera estática, incluida la capacidad para ofrecer soporte a redes cambiantes. Sólo se cede a los clientes las direcciones IP, de manera que, cuando ya no la necesitan o se desplazan a otra subred, la dirección puede ser LIBERADA y quedar a disposición de otros clientes para que la utilicen.

Operación DHCP

DHCP permite a los clientes obtener información de configuración de red IP, incluida una dirección IP, de un servidor DHCP central. Los servidores DHCP controlan si las direcciones que proporcionan a clientes se asignan de manera permanente o se ceden durante un periodo específico de tiempo. Cuando un cliente recibe una dirección cedida, debe solicitar de manera periódica que el servidor revalide la dirección y renueve la cesión.

Todos los procesos de asignación de direcciones, cesión y renovación de la cesión son gestionados por el cliente DHCP y los programas del servidor y son transparentes para los usuarios finales. Los clientes utilizan mensajes con la arquitectura RFC para aceptar y utilizar las opciones que les sirve el servidor DHCP. Por ejemplo:

1. El cliente difunde un mensaje (que contiene su ID de mensaje) 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 del dominio y la ruta estática.

2. De manera opcional, si los direccionadores de la red están configurados para reenviar mensajes DHCP y BOOTP (mediante BOOTP Relay), el mensaje de difusión se reenvía a los servidores DHCP de las redes conectadas.
3. Cada servidor DHCP que recibe el mensaje DHCPDISCOVER del cliente envía un mensaje de DHCPOFFER al cliente ofreciéndole una dirección IP. El servidor DHCP comprueba la existencia de direcciones IP en la red antes de emitir una oferta. Así mismo, comprueba el archivo de configuración para saber si debe asignar una dirección estática o dinámica a este cliente. En el caso de una dirección dinámica, el servidor selecciona una dirección de la agrupación de direcciones, eligiendo la que hace más tiempo que se ha utilizado. Una agrupación de direcciones es un rango de direcciones IP que deben cederse a clientes. En el caso de una dirección estática, el servidor utiliza una sentencia Client de la configuración del servidor DHCP para asignar opciones a los clientes. Una vez se ha efectuado la oferta, el servidor DHCP reserva la dirección ofrecida.
4. El cliente recibe los mensajes de oferta y selecciona el servidor que desea utilizar. Cuando un cliente DHCP recibe una oferta, toma nota de cuántas opciones de las solicitadas se han incluido en la oferta. El cliente DHCP continúa recibiendo ofertas de los servidores DHCP durante un intervalo de 4 segundos después de que se reciba la primera oferta, tomando nota de cuántas opciones de las solicitadas se han incluido en cada oferta. Cuando finaliza este intervalo, el cliente DHCP compara todas las ofertas y selecciona la que satisface sus criterios.
5. El cliente difunde un mensaje para indicar el servidor que ha seleccionado y el uso de las peticiones de la dirección IP ofrecida por dicho servidor (mensaje DHCPREQUEST).
6. Si un servidor recibe un mensaje DHCPREQUEST que indica que el cliente ha aceptado la oferta del servidor, el servidor marca dicha dirección como cedida. Si el servidor recibe un mensaje DHCPREQUEST que indica que el cliente ha aceptado una oferta de un servidor diferente, el servidor devuelve la dirección a la agrupación disponible. Si no se recibe ningún mensaje dentro de un tiempo especificado, el servidor devuelve la dirección a la agrupación disponible. El servidor seleccionado envía un reconocimiento que contiene información de configuraciones adicionales al cliente (mensaje DHCPACK).
7. El cliente determina si la información de configuración es válida. Una vez se ha recibido un mensaje DHCPACK, los clientes DHCP envían una petición de protocolo de resolución de direcciones (ARP) a la dirección IP suministrada para comprobar si ésta ya está en uso. Si recibe una respuesta a la petición ARP, el cliente declina (mensaje DHCPDECLINE) la oferta e inicia el proceso de nuevo. De lo contrario, el cliente acepta la información de configuración.
8. Al aceptar una cesión válida, el cliente entra en un estado de ENLACE con el servidor DHCP y procede a la utilización de la dirección y las opciones IP. Si el cliente DHCP es un cliente de direcciones dinámicas, el cliente DHCP notifica el servidor de nombres de dominio dinámico de su correlación de nombre de sistema principal con dirección IP.

Para los clientes DHCP que solicitan opciones, el servidor DHCP habitualmente proporciona opciones tales como la máscara de subred, el servidor de nombres de dominio, el nombre de dominio, la ruta estática, el identificador de clase (que identifica a un proveedor concreto) y la clase de usuario.

De todos modos, un cliente DHCP puede solicitar su propio juego exclusivo de opciones. Por ejemplo, es obligatorio que los clientes DHCP de Windows NT 3.5.1

soliciten opciones. El juego de opciones DHCP solicitadas por omisión que IBM proporciona está formado por la máscara de subred, el servidor de nombres de dominio, el nombre de dominio y la ruta estática. Si desea obtener descripciones de las opciones, consulte “Opciones DHCP” en la página 487.

Renovaciones de cesiones

El cliente DHCP hace un seguimiento del tiempo de cesión restante. En un momento especificado anterior a la finalización de la cesión, normalmente cuando ha transcurrido la mitad del tiempo de cesión, el cliente envía al servidor de cesiones una petición de renovación que contiene su dirección IP actual e información de configuración. Si el servidor responde con una oferta de cesión, la cesión del cliente DHCP se renueva.

Si el servidor DHCP rechaza explícitamente la petición, el cliente DHCP puede continuar utilizando la dirección IP hasta que el tiempo de cesión finaliza e iniciar, a partir de entonces, el proceso de petición de direcciones, incluida la difusión de la petición de direcciones. Si no se puede acceder al servidor, el cliente puede continuar utilizando la dirección asignada hasta que la cesión finalice.

Movimiento del cliente

Uno de los beneficios de DHCP es la libertad que proporciona a un sistema principal cliente para moverse de una subred a otra sin tener que estar al corriente previamente de la información de configuración que necesita en la nueva subred. En la medida que las subredes a las que un sistema principal reubica disponen de acceso a un servidor DHCP, un cliente DHCP se configurará correctamente a sí mismo de manera automática para acceder a dichas subredes.

A fin de que los clientes DHCP se vuelvan a configurar para acceder a una nueva subred, se debe volver a arrancar el sistema principal cliente. Cuando un sistema principal se reinicia en una nueva subred, los clientes DHCP intentan renovar la antigua cesión con el servidor DHCP que originalmente asignó la dirección. El servidor rechaza la renovación de la petición ya que la dirección no es válida en la nueva subred. Al no recibir respuesta o instrucciones del servidor DHCP, el cliente inicia el proceso de petición de dirección IP para obtener una nueva dirección IP y acceder a la red.

Modificación de las opciones de servidor

Con el DHCP, se pueden efectuar cambios en el servidor, reinicializar el servidor y distribuir los cambios a todos los clientes adecuados. Un cliente DHCP retiene los valores de opciones DHCP asignados por el servidor DHCP mientras dure la cesión. Si se implementan modificaciones de configuración en el servidor mientras un cliente ya está activo y en funcionamiento, el cliente DHCP no procesa dichas modificaciones hasta que los clientes intentan renovar su cesión o hasta que se reinician.

Nota: Si el servidor se reinicializa (mediante el mandato `t 5` **reset dhcp**), la información de tiempo de cesión que el direccionador visualiza se perderá hasta que los clientes DHCP renueven su cesión.

Número de servidores DHCP

El número de servidores necesario dependerá en gran medida del número de subredes de que disponga, del número de clientes DHCP a los que prevea ofrecer soporte, de si utiliza el BOOTP Relay, y del tiempo de cesión que elija. Recuerde que el protocolo DHCP no define actualmente comunicación de servidor a servidor. Por lo tanto, no pueden compartir información, ni uno de los servidores DHCP puede actuar como una “copia de seguridad dinámica” en el caso de que el otro falle. Los clientes DHCP envían mensajes de difusión. Por diseño, los mensajes de difusión no cruzan subredes. Para que los mensajes del cliente se puedan reenviar fuera de su subred, se deben configurar direccionadores adicionales para reenviar peticiones DHCP mediante el agente de BOOTP Relay. De lo contrario, será necesario configurar un servidor DHCP en cada subred.

Un único servidor DHCP

Si decide utilizar un único servidor DHCP para servir a sistemas principales en un subred, tenga en cuenta los efectos que puede tener el hecho de que dicho servidor falle. Por lo general, la anomalía de un servidor afectará sólo a los clientes DHCP que están intentando unirse a la red. En principio, los clientes DHCP que ya se hallan en la red continuarán funcionando sin verse afectados hasta que finalice la cesión. De todos modos, los clientes que dispongan de un tiempo de cesión bajo pueden perder su acceso de red antes de que el servidor se pueda reiniciar. Para minimizar el impacto del tiempo de inactividad del servidor si sólo dispone de un servidor DHCP para una subred, deberá elegir un tiempo de cesión lo suficientemente largo como para permitir que haya tiempo para reiniciar o responder al servidor DHCP que ha fallado.

Varios servidores DHCP

Para evitar un único punto de anomalía, puede configurar dos o más servidores DHCP para servir a la misma subred. Si un servidor falla, el otro puede continuar sirviendo a la subred. Se debe poder acceder a cada uno de los servidores DHCP mediante conexión directa a la subred o utilizando un agente BOOTP Relay.

Como dos servidores DHCP no pueden servir las mismas direcciones, las agrupaciones de direcciones definidas para una subred deben ser exclusivas entre los servidores. Por lo tanto, cuando se utilizan dos o mas servidores DHCP para servir a una subred en concreto, la lista completa de direcciones de dicha subred debe dividirse entre los servidores. Por ejemplo, puede configurar un servidor con una agrupación de direcciones que contenga un 70% de las direcciones disponibles para la subred y el otro servidor con una agrupación de direcciones que contenga el 30% restante de las direcciones disponibles.

Al utilizar varios servidores DHCP se reduce la probabilidad de sufrir una anomalía de acceso de red relacionada con DHCP pero su utilización no representa garantía alguna ante tal anomalía. Si un servidor DHCP de una subred en concreto falla, es probable que el otro servidor DHCP no pueda atender a todas las peticiones de los nuevos clientes que pueden, por ejemplo, agotar la agrupación limitada de direcciones disponibles del servidor.

De todos modos, puede desviar el servidor que agotará en primer lugar su agrupación de direcciones. Los clientes DHCP tienden a seleccionar el servidor DHCP que ofrece más opciones. Para desviar el servicio hacia el servidor DHCP con el 70% de direcciones disponibles, deberá ofrecer menos opciones DHCP del servidor que posee el 30% de direcciones disponibles para la subred.

Servidores BOOTP

Si ya dispone de clientes y servidores BOOTP en la red, es probable que desee considerar la posibilidad de sustituir los servidores BOOTP por servidores DHCP. Los servidores DHCP pueden servir de manera opcional a clientes BOOTP la misma información de configuración IP que los servidores BOTTP actuales. Si no puede sustituir los servidores BOOTP por servidores DHCP y desea que ambos sirvan en la red, se recomienda adoptar las siguientes medidas de precaución:

- Desactivar el soporte BOOTP en el servidor DHCP.
- Asegurarse de que los servidores BOOTP y los servidores DHCP no distribuyen las mismas direcciones.
- Configurar el soporte de BOOTP Relay en los direccionadores para reenviar difusiones BOOTP tanto a los servidores BOOTP como a los servidores DHCP adecuados.

Un servidor DHCP asigna una dirección IP permanente a un cliente BOOTP. En el caso de que las subredes se vuelvan a numerar de modo que un BOOTP asignado no se pueda volver a utilizar, el cliente BOOTP se deberá reiniciar y deberá obtener una nueva dirección IP.

Clientes DHCP especiales

Es probable que disponga de clientes DHCP o de servidores de red que tengan necesidades administrativas individuales o especiales como, por ejemplo:

- Una cesión permanente:

  Puede asignar cesiones permanentes para designar sistemas principales especificando un tiempo de cesión infinito. El servidor DHCP también asignará una cesión permanente a los clientes BOOTP que lo soliciten de manera explícita en la medida en que el soporte para clientes BOOTP esté habilitado. El servidor DHCP también asignará una cesión permanente a sistemas principales DHCP que lo soliciten de manera explícita.
- Una dirección IP específica:

  Puede reservar una dirección específica y parámetros de configuración para un sistema principal cliente DHCP o BOOTP de una subred concreta.
- Parámetros de configuración específicos:

  Puede asignar información de configuración específica a un cliente sin tener en cuenta su subred.
- Estaciones de trabajo definidas manualmente:

  Debe excluir de forma explícita de las subredes DHCP las direcciones de sistemas principales existentes que no utilizan DHCP o BOOTP para configurar su acceso de red IP. Aunque los servidores y clientes DHCP comprueban de manera automática si hay una dirección IP en uso antes de asignarla o utilizarla, éstos no podrán detectar direcciones de sistemas principales definidos manualmente que estén desactivados o que estén temporalmente fuera de red. En tal caso, se pueden duplicar los problemas con las direcciones en el momento en que un sistema definido manualmente vuelva a acceder a la red, a menos que su dirección IP sea excluida de manera explícita.

Tiempos de cesión

El tiempo de cesión por omisión es de 24 horas. Recuerde que el tiempo de cesión DHCP puede afectar al funcionamiento y al rendimiento de la red:

- Los tiempos de cesión cortos aumentan la cantidad de tráfico de red debido a las peticiones de renovaciones de cesión DHCP. Por ejemplo, si establece un tiempo de cesión de 5 minutos, cada cliente envía una petición de renovación aproximadamente cada 2,5 minutos.
- Los tiempos de cesión que son demasiado largos pueden limitar la capacidad de reutilización de las direcciones IP. Los tiempos de cesión muy largos también retrasan los cambios en la configuración que se producen cuando un cliente reinicia o renueva una cesión.

El tiempo de cesión que elija dependerá en gran media de sus necesidades, entre las que se cuentan:

- El número de sistemas principales a los que se debe ofrecer soporte comparado con el número de direcciones disponibles. Si tiene más sistemas principales que direcciones, es probable que desee seleccionar un tiempo de cesión corto de una o dos horas. Ello le ayudará a garantizar que las direcciones que no se utilicen se devuelvan a la agrupación lo antes posible.
- El tiempo disponible para realizar cambios de red. Los sistemas principales reciben cambios en la información de configuración cuando se reinician o renuevan su cesión. Asegúrese de que una ventana adecuada y oportuna pueda efectuar dichos cambios. Por ejemplo, si normalmente efectúa cambios durante la noche, puede asignar un tiempo de cesión de 12 horas.
- El número de servidores DHCP que están disponibles. Si dispone sólo de unos pocos servidores DHCP para una red grande, es probable que desee seleccionar un tiempo de cesión más largo para minimizar el impacto del tiempo de inactividad del servidor.

Para redes complejas que necesitan ofrecer soporte a una combinación de requisitos de cesión de sistemas principales se pueden definir las clases DHCP.

Conceptos y terminología

Los siguientes conceptos se utilizan para describir las funciones del servidor DHCP:

Ámbito

El término ámbito, cuando se habla de configuración del servidor DHCP, se utilizará para identificar aquello a lo que pertenece un determinado valor de parámetro. La Figura 46 en la página 485 ilustra los siguientes ámbitos:

- Opción global 1
- Opción global 3
- Clase global ClassA

  ClassA ha redefinido la opción 1 pero heredará el valor de la opción 3 del ámbito global.
- Cliente global ClientA

  ClientA 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 ClassA dentro del ámbito de SubA.

Redefine el valor de la opción 1 pero heredará el valor de la opción 3 de SubA (que también heredará del ámbito global).

— Define ClientB dentro del ámbito SubA.

ClientB ha redefinido la opción 3 pero heredará el valor de la opción 1 de SubA.

- Opción de proveedor vendorA

Las opciones de proveedor son una excepción. Las opciones de proveedor son independientes y no se heredan fuera del ámbito de opción de proveedor.

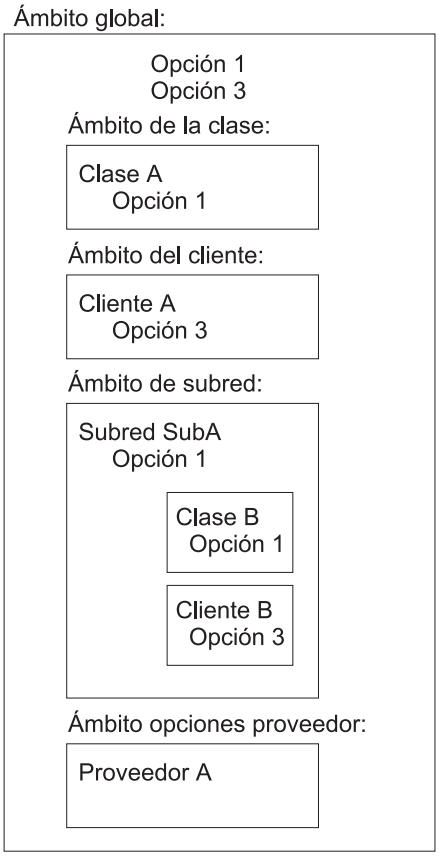


Figura 46. Conceptos de ámbito

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 deben cederse a clientes. Los parámetros que se pueden especificar son el tiempo de cesión y otras opciones para clientes que utilicen la agrupación de direcciones. El tiempo de cesión y otras opciones se pueden heredar del ámbito global.

Grupos de subredes

Un grupo de subredes es una manera de identificar varias subredes que se deben agrupar en la misma interfaz. A todas las subredes de un grupo

determinado se les concede el mismo nombre de grupo de subredes y una prioridad exclusiva. La prioridad se utiliza para determinar el orden en que se distribuyen las direcciones según la política de direcciones a la que está asociado el grupo. Una subred puede pertenecer a una o dos políticas de direcciones:

- Inorder

  Esta política es el valor por omisión. La política en servicio administra las direcciones empezando con la subred que tiene la prioridad más baja y acabando con la subred que tiene la prioridad más alta.

- Balance

  La política de equilibrio administra las direcciones del grupo de subredes definidas siguiendo un orden rotatorio. La primera dirección es administrada desde la subred con la prioridad más baja. La segunda dirección es administrada desde la subred con la siguiente prioridad más baja y así sucesivamente. Cuando se ha administrado una dirección de la subred de mayor prioridad, la política vuelve a la subred con menor prioridad hasta que todas las direcciones de todas las subredes del grupo se han agotado.

Clases Una clase define los parámetros de un grupo de clientes definido por el usuario y que es administrado por el servidor DHCP. Las clases se pueden definir bajo el ámbito global o de una subred. Cuando una clase se define dentro del ámbito de una subred, el servidor DHCP sólo servirá a clientes de la clase que estén ubicados en la subred especificada y a la vez soliciten la clase. Sólo las clases que se definen dentro de un ámbito de subred pueden especificar un rango de direcciones. El rango puede ser una subred del rango de subredes o puede ser equivalente al rango de subredes. A un cliente que solicita una dirección IP de una clase que ha agotado su rango se le ofrece una dirección IP del rango de subred, si está disponible. Al cliente se le ofrecen las opciones asociadas con la clase agotada.

Clientes

Un cliente se puede utilizar para:

- Definir una dirección IP y opciones 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 específicos. Los tipos de hardware se definen en RFC 1340 y se muestran a continuación. Para todos los tipos de hardware excepto 0, el ID de cliente es la dirección de hardware de la estación final (o la dirección MAC). Para el tipo de hardware 0, el id de cliente es una cadena de caracteres. Habitualmente se trata de un nombre de dominio.

Cuando se define un cliente, se le solicita una dirección IP *cualquiera* o *ninguna*. Si define una dirección IP, dicha dirección IP se reserva para ese cliente. Si elige *cualquiera*, a ese cliente se le concederá cualquier dirección IP disponible dentro de esa subred. Si dispone de bastantes registros de subred definidos dentro de la misma subred, cada uno de los cuales con un rango exclusivo, un cliente que esté configurado con *cualquiera* obtendrá la primera dirección disponible dentro de la subred, no necesariamente del rango del registro de subred específico bajo el que está definido el cliente. Si elige *ninguna*, a esa estación final no se le servirá dirección IP alguna.

Para excluir la posibilidad de administrar una dirección IP, debería definir un registro de cliente con un tipo de hardware e id de cliente 0.

Los tipos de hardware que RFC1340 define y que pertenecen al IBM 2212 son:

Hardware Type	Value
Reserved	0
Ethernet	1
IEEE 802 Networks (including Token Ring)	6

Si desea obtener una lista completa, consulte RFC 1340.

Parámetros de servidor DHCP y de cesión

Los siguientes parámetros de servidor DHCP se pueden definir 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 532 si desea obtener una descripción de dichos parámetros.

Opciones DHCP

DHCP permite especificar opciones para proporcionar información de configuración adicional a un cliente. Las opciones se definen en RFC 2132 y en varios RFC más.

Formatos de opción

Todas las opciones esperan que los datos de configuración estén en uno de los siguientes formatos:

Formato	Definición
Dirección IP	Una única dirección IP en notación decimal por puntos.
Direcciones IP	Una o más direcciones IP en notación decimal por puntos, separadas por espacios en blanco.
Par de direcciones IP	Dos direcciones IP en notación decimal por puntos, separadas por espacios en blanco.
Pares de direcciones IP	Un o varios pares de direcciones IP, cada uno de ellos separado del otro por un espacio en blanco.
Booleano	0 o 1 (Verdadero o falso).
Byte	Un número decimal entre -128 y 127 (ambos incluidos).

Byte no firmado	Un número decimal entre 0 y 255 (ambos incluidos). No se puede especificar un valor negativo para un byte no firmado.
Lista de bytes no firmados	Uno o más números decimales entre 0 y 255 (ambos incluidos) separados por espacios en blanco. No se puede especificar un número negativo para un byte no firmado.
Corto	Un número decimal entre -32768 y 32767 (ambos incluidos).
Corto no firmado	Un número decimal entre 0 y 65535 (ambos incluidos). No se puede especificar un número negativo para un corto no firmado.
Lista de cortos no firmados	Uno o más números decimales entre 0 y 65535 (ambos incluidos) separados por espacios en blanco. No se puede especificar un número negativo para un corto no firmado.
Largo	Un número decimal entre -2147483648 y 2147483647 (ambos incluidos).
Largo no firmado	Un número decimal entre 0 y 4294967295 (ambos incluidos). No se puede especificar un número negativo para un largo no firmado.
Cadena	Una cadena de caracteres.
D/N	Indica que no es necesaria especificación alguna porque el cliente genera esta información.

Cada opción DHCP se identifica mediante un código numérico.

Las opciones de la arquitectura de la 0 a la 127 y la opción 255 están reservadas para definiciones efectuadas por RFC. El servidor DHCP, el cliente DHCP o ambos utilizan las opciones de ese conjunto. El administrador puede modificar algunas opciones de la arquitectura. Otras opciones son para uso exclusivo del cliente y del servidor.

Nota: No se permiten valores hexadecimales para opciones de la arquitectura con formatos conocidos.

Las opciones que el administrador no puede o no debe configurar en el servidor DHCP son:

52 Carga de opciones

53 Tipo de mensaje 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 de la 128 a la 254 son opciones definidas por el usuario que los administradores pueden definir para pasar información al cliente DHCP a fin de implementar 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, excepto los códigos que ya están definidos en un RFC.

valor Debe ser siempre una cadena de caracteres. En el servidor puede ser una cadena ASCII o una cadena hexadecimal. En el cliente, sin embargo, aparece siempre como una cadena hexadecimal cuando pasa al programa de proceso.

El servidor pasa el valor especificado al cliente. De todos modos, se debe crear un archivo de programa o de mandatos para procesar el valor.

Opciones base proporcionadas al cliente

Las siguientes opciones base se proporcionan al cliente. Consulte “Formatos de opción” en la página 487 si desea obtener 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 se especifica en notación decimal por puntos de 32 bits. Aunque no es obligatorio, en la mayoría de configuraciones el servidor DHCP debe enviar la opción 1, la máscara de subred, a los clientes DHCP. El funcionamiento del cliente puede ser impredecible si el cliente no recibe ninguna máscara de subred del servidor DHCP y presupone que existe 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 la opción: Direcciones IP

2 **Diferencia horaria** Esta opción se especifica sólo en el servidor DHCP. La diferencia (en segundos) de la subred del cliente con la Coordinated Universal Time (CUT). La diferencia es un entero de 32 bits firmado.

Formato de la opción: Largo

3 **Direccionador** Esta opción sólo se especifica en el servidor DHCP. Las direcciones IP (en orden de preferencia) de los direccionadores de la subred del cliente.

Formato de la opción: Direcciones IP

4 **Servidor horario** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (en orden de preferencia) de los servidores horarios disponibles para el cliente.

Formato de la opción: Direcciones IP

5 **Servidor de nombres** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (en orden de preferencia) de los servidores de nombres IEN 116 disponibles para el cliente.

Nota: No es la opción Servidor de nombres de dominio. Utilice la opción 6 para especificar un servidor de nombres de dominio.

Formato de la opción: Direcciones IP

6 **Servidor de nombres de dominio** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (en orden de preferencia) de los servidores del Sistema de nombres de dominio disponibles para el cliente.

Formato de la opción: Direcciones IP

Nota: Si se ha configurado una dirección dinámica en una interfaz PPP, podrá recuperar una dirección DNS primaria y una secundaria mediante el IPCP de un proveedor de servicios de Internet (ISP). Para pasar estas direcciones DNS a los clientes DHCP en la opción 6, debe configurar una dirección de interfaz IP no numerada (como 0.0.0.n) que corresponda a la interfaz de dirección dinámica. El servidor DHCP convertirá dicho valor en las direcciones que se recuperen cuando el cliente envíe una petición. Si el cliente DHCP ha solicitado su información de configuración al servidor antes de que se active la interfaz PPP, el cliente deberá reiniciar o renovar su cesión para recibir las direcciones DNS averiguadas.

7 **Servidor de anotaciones** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (en orden de preferencia) de los servidores de anotaciones MIT-LCS UDP disponibles para el cliente.

Formato de la opción: Direcciones IP

8 **Servidor de cookies** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (en orden de preferencia) de la Cookie o los servidores "cita del día" disponibles para el cliente.

Formato de la opción: Direcciones IP

9 **Servidor LPR** Esta opción se puede especificar tanto en el cliente DHCP como en el servidor DHCP. No obstante, si se especifica sólo en el cliente DHCP, la configuración será incompleta. Las direcciones IP (en orden de preferencia) de los servidores de impresoras de línea disponibles para el cliente. La opción 9 elimina la necesidad de que los clientes especifiquen la variable de entorno LPR_SERVER.

Formato de la opción: Direcciones IP

10 **Servidor Impress** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (en orden de preferencia) de los servidores Imagen Impress disponibles para el cliente.

Formato de la opción: Direcciones IP

11 **Servidor de ubicación de recursos** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (en orden de preferencia) de los servidores Resource Location (RLP) disponibles para el cliente. Los servidores RLP permiten que los clientes ubiquen los recursos que proporcionan un servicio determinado como puede ser un servidor de nombres de dominio.

Formato de la opción: Direcciones IP

12 **Nombre del sistema principal** Esta opción se puede especificar tanto en el cliente DHCP como en el servidor DHCP. Si el cliente DHCP no proporciona un nombre de sistema principal, el servidor DHCP ignora la

opción 12. El nombre del sistema principal del cliente (que puede incluir el nombre de dominio local). La longitud mínima del nombre del sistema principal es 1 octeto y la máxima es 32 caracteres. Consulte RFC 1035 si desea conocer las restricciones de juegos de caracteres.

Formato de la opción: Cadena de caracteres

13 **Tamaño del archivo de arranque** Esta opción se especifica sólo en el servidor DHCP. El tamaño (en bloques de 512 octetos) del archivo de configuración de arranque del cliente.

Formato de la opción: Corto no firmado.

14 **Archivo de vuelco de mérito** Esta opción se especifica sólo en el servidor DHCP. El nombre de la vía de acceso del archivo de vuelco de mérito en el que la imagen de memoria del cliente se almacena si el cliente cae. La vía de acceso tiene el formato de una cadena de caracteres del juego de caracteres de terminal virtual de redes (NVT) ASCII. La longitud mínima es 1 octeto.

Formato de la opción: Cadena de caracteres

15 **Nombre de dominio** Esta opción se especifica tanto en el cliente DHCP como en el servidor DHCP. Si no se especifica ningún valor en el servidor DHCP en la opción 15, se solicita al cliente que proporcione un valor para la opción 12, nombre del sistema principal, y para la opción 15, nombre de dominio. Esta sentencia puede aparecer dentro del ámbito global o con un ámbito de Subred, Clase o Cliente.

Formato de la opción: Cadena de caracteres

16 **Servidor de intercambio** Esta opción se especifica sólo en el servidor DHCP. La dirección IP del servidor de intercambio del cliente.

Formato de la opción: Dirección IP

17 **Vía de acceso 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 tiene el formato de una cadena de caracteres del juego de caracteres NVT ASCII. La longitud mínima es 1 octeto.

Formato de la opción: Cadena de caracteres

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 cadena de caracteres que se puede utilizar para identificar un archivo que se puede recuperar mediante el protocolo de transferencial de archivos trivial (TFTP). La longitud mínima es 1 octeto.

Formato de la opción: Cadena de caracteres

Parámetros de capa IP por opciones de sistema principal

19 **Reenvío IP** Esta opción se especifica sólo en el servidor DHCP. Habilita (1) o inhabilita (0) el reenvío por parte del cliente de sus paquetes de capa IP.

Formato de la opción: Booleano

20 **Direccionamiento de orígenes no locales** Esta opción se especifica sólo en el servidor DHCP. Habilite (1) o inhabilite (0) el reenvío por parte del cliente de sus datagramas de capa IP con rutas de orígenes no locales.

Formato de la opción: Booleano

21 **Filtro de política** Esta opción se especifica sólo en el servidor DHCP. El par de máscaras de dirección IP-red que se utiliza para filtrar datagramas con rutas de orígenes no locales. Cualquier datagrama cuya siguiente dirección de salto no coincide con uno de los pares de filtros es descartado por el cliente. La longitud mínima de la opción de filtro de política es 8 octetos.

Formato de la opción: Pares de direcciones IP

22 **Tamaño máximo de reensamblaje de datagramas** Esta opción se especifica sólo en el servidor DHCP. El datagrama de tamaño máximo que el cliente reensamblará. El valor mínimo es 576.

Formato de la opción: Corto no firmado.

23 **Tiempo de vida IP por omisión** Esta opción se especifica sólo en el servidor DHCP. El tiempo de vida (TTL) por omisión que el cliente utiliza en los datagramas salientes. TTL es un octeto con un valor entre 1 y 255.

Formato de la opción: Byte no firmado

24 **Tiempo de espera de antigüedad de Path MTU** Esta opción se especifica en el servidor DHCP. El tiempo de espera en segundos para establecer la antigüedad de los valores de la unidad de transmisión máxima (MTU) de vía de acceso descubiertos por el mecanismo que se describe en RFC 1191.

Formato de la opción: Largo no firmado

25 **Tabla plana de Path MTU** Esta opción se especifica sólo en el servidor DHCP. La tabla de tamaños de MTU a reclamar en el descubrimiento de la Path MTU tal como se define en RFC 1191. El valor mínimo de MTU es 68. La longitud mínima de la opción de tabla plana de la Path MTU es 2 octetos. La longitud debe ser un múltiplo de 2.

Formato de la opción: Corto no firmado.

Parámetros de capa IP por opciones de interfaz

26 **MTU de interfaz** Esta opción se especifica sólo en el servidor DHCP. La unidad de transmisión máxima (MTU) a presentar en esta interfaz. El valor de MTU mínimo es 68.

Formato de la opción: Corto no firmado.

27 **Todas las subredes son locales** Esta opción se especifica sólo en el servidor DHCP. El cliente presupone (1) o no presupone (0) que todas las subredes utilizan la misma unidad de transmisión máxima (MTU). Un valor de 0 significa que el cliente presupone que algunas subredes tienen MTU más pequeñas.

Formato de la opción: Booleano

28 **Dirección de difusión** Esta opción se especifica sólo en el servidor DHCP. La dirección de difusión que se utiliza en la subred del cliente.

Formato de la 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 la máscara de subred mediante el protocolo de mensajes de control de Internet (ICMP).

Formato de la opción: Booleano

30 **Proveedor de máscaras** 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 de mensajes de control de Internet (ICMP).

Formato de la opción: Booleano

31 **Realizar descubrimiento de direccionadores** Esta opción se especifica sólo en el servidor DHCP. El cliente solicita (1) o no solicita (0) direccionadores mediante el descubrimiento de éstos tal y como se define en RFC 1256.

Formato de la opción: Booleano

32 **Dirección de solicitación de direccionadores** Esta opción se especifica sólo en el servidor DHCP. La dirección a la que un cliente transmite las peticiones de solicitación de direccionadores.

Formato de la opción: Dirección IP

33 **Ruta estática** Esta opción se especifica sólo en el servidor DHCP. Las rutas estáticas (los pares de direcciones-direccionadores de designación en orden de preferencia) que el cliente instala en su antememoria de direccionamiento. La primera dirección es la dirección de destino y la segunda dirección es el direccionador de destino. No especifique 0.0.0.0 como destino de ruta por omisión.

Formato de la opción: Pares de direcciones IP

Parámetros de capa de enlace por opciones de interfaz

34 **Encapsulación de rastreadores** Esta opción se especifica sólo en el servidor DHCP. El cliente negocia (1) o no negocia (0) el uso de rastreadores al utilizar el protocolo de resolución de direcciones (ARP). Si desea obtener más información, consulte RFC 893.

Formato de la opción: Booleano

35 **Tiempo de espera de la antememoria ARP** Esta opción se especifica sólo en el servidor DHCP. El tiempo de espera en segundos para las entradas de antememoria del protocolo de resolución de direcciones (APR).

Formato de la opción: Largo no firmado

36 **Encapsulación de Ethernet** Esta opción se especifica sólo en el servidor DHCP. Para una interfaz Ethernet, el cliente utiliza la encapsulación de Ethernet IEEE 802.3 (1) descrita en RFC 1042 o la encapsulación de Ethernet V2 (0) descrita en RFC 894.

Formato de la opción: Booleano

Opciones de parámetros TCP

37 **TTL por omisión de TCP** Esta opción se especifica sólo en el servidor DHCP. El tiempo de vida (TTL) por omisión que el cliente utiliza para enviar segmentos de TCP.

Formato de la opción: Byte no firmado

38 **Intervalo de mantenimiento de la actividad de TCP** Esta opción se especifica sólo en el servidor DHCP. Intervalo en segundos que el cliente espera antes de enviar un mensaje de mantenimiento de la actividad en

una conexión de TCP. Un valor 0 indica que el cliente no envía mensajes de mantenimiento de la actividad a menos que la aplicación lo solicite.

Formato de la opción: Largo no firmado

39 **Basura de mantenimiento de la actividad de TCP** Esta opción se especifica sólo en el servidor DHCP. El cliente envía (1) o no envía (0) mensajes de mantenimiento de la actividad de TCP que contienen un octeto desechable para alcanzar la compatibilidad con implementaciones anteriores.

Formato de la opción: Booleano

Opciones de parámetros de aplicaciones y servicios

40 **Dominio del servicio de información de red** Esta opción se especifica sólo en el servidor DHCP. El dominio del servicio de información de red (NIS) del cliente. El dominio tiene el formato de un cadena de caracteres del juego de caracteres NVT ASCII. La longitud mínima es 1 octeto.

Formato de la opción: Cadena de caracteres

41 **Dominio del servicio de información de red** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (en orden de preferencia) de los servidores de servicio de información de red (NIS) disponibles para el cliente.

Formato de la opción: Direcciones IP

42 **Servidores de protocolo horario de red** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (en orden of preferencia) de los servidores de protocolo horario de red (NTP) disponibles para el cliente.

Formato de la opción: Direcciones IP

43 **Información específica del proveedor** La opción 43 se especifica sólo en el servidor DHCP, que la devuelve a un cliente que envía la opción 60, Identificador de clase. Esta opción de información es utilizada por clientes y servidores para intercambiar información específica de proveedores, que se especifica en la definición de opción de proveedores. Los siguientes aspectos se deben tener en cuenta al utilizar la opción 43 para encapsular información de proveedores:

- Para permitir la interoperabilidad entre clientes y servidores de diferentes proveedores, cada proveedor debe documentar de forma clara el contenido de su respectiva opción 43 mediante el formato estándar de RFC 2132.
- Cada proveedor debe especificar las opciones concretas que se pueden encapsular dentro de la opción 43 de forma que los servidores DHCP de otro proveedor puedan implementarlas fácilmente. Por ejemplo, el proveedor deberá:
  - — Representar dichas opciones en tipos de datos ya definidos para las opciones DHCP o en otros tipos de datos definidos públicamente.
  - — Elegir opciones que se puedan codificar rápidamente en archivos de configuración para su intercambio con servidores suministrados por otros proveedores.
  - — Poder recibir rápidamente el soporte de todos los servidores.

Los servidores que no pueden interpretar la información específica del proveedor enviada por un cliente deben ignorarla. Los clientes que no reciban las información específica del proveedor deseada deben intentar operar sin ella. Consulte RFC 2131 y RFC 2132 si desea obtener información adicional sobre esta opción.

Nota: Debido a las consideraciones anteriores, IBM utiliza, en cambio, las opciones 192 y 200 como sus opciones específicas.

Formato de la opción: Cadena de caracteres

44 **NetBIOS en el servidor de nombres TCP/IP** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (en orden de preferencia) de los servidores de nombres NetBIOS (NBNS) disponibles para el cliente.

Formato de la opción: Direcciones IP

45 **NetBIOS en el servidor de distribución de datagramas TCP/IP** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (en orden de preferencia) de los servidores de nombres de distribución de datagramas del NetBIOS (NBDD) disponibles para el cliente.

Formato de la opción: Direcciones IP

46 **NetBIOS en el tipo de nodo TCP/IP** Esta opción se especifica sólo en el servidor DHCP. El tipo de nodo utilizado para el NetBIOS en los clientes configurables TCP/IP tal y como se describe en RFC 1001 y RFC 1002. Los valores para especificar los tipos de clientes son:

- 0x1 nodo B
- 0x2 nodo P
- 0x4 nodo M
- 0x8 nodo H

Formato de la opción: Byte no firmado

47 **NetBIOS en ámbito TCP/IP** Esta opción se especifica sólo en el servidor DHCP. El parámetro de NetBIOS en ámbito TCP/IP, tal y como se especifica en RFC 1001/1002. La longitud mínima es 1 octeto.

Formato de la opción: Byte no firmado

48 **Servidor de fonts del sistema X Window** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (en orden of preferencia) de los servidores de fonts del sistema X Window disponibles para el cliente.

Formato de la opción: Direcciones IP

49 **Gestor de visualización del sistema Window** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (en orden de preferencia) de los sistemas que ejecutan el Gestor de visualización del sistema X Window disponible para el cliente.

Formato de la opción: Direcciones IP

Opciones de extensiones DHCP

50 **Dirección IP solicitada** Esta opción se especifica sólo en el cliente DHCP. El servidor DHCP puede rechazar la petición de una dirección IP específica por parte de un cliente DHCP. Esta opción permite al cliente solicitar una dirección IP concreta (DHCPDISCOVER).

Formato de la opción: D/N

51 **tiempo de cesión de direcciones IP** Esta opción se puede especificar tanto en el cliente DHCP como en el servidor DHCP. El cliente DHCP puede utilizar la opción 51 para alterar el valor defaultLeaseInterval que el servicio ofrece. Permite al cliente solicitar (DHCPDISCOVER o DHCPREQUEST) un tiempo de cesión para una dirección IP. En una respuesta (DHCPOFFER), un servidor DHCP utiliza la opción para ofrecer un tiempo de cesión. Esta opción se puede especificar dentro del ámbito global, de subred, de clase o de cliente. Utilice X'ffffffff' para indicar una cesión infinita (permanente).

Formato de la opción: Largo no firmado

58 **Valor de tiempo de renovación (T1)** Esta opción se especifica sólo en el servidor DHCP. El intervalo en segundos que transcurre entre el momento en que el servidor asigna una dirección y el momento en que el cliente pasa a estado de renovación.

Formato de la opción: Largo no firmado

59 **Valor de tiempo de reenlace (T2)** Esta opción se especifica sólo en el servidor DHCP. El intervalo en segundos que transcurre entre el momento en que el servidor asigna una dirección y el momento en que el cliente entra en estado de reenlace.

Formato de la opción: Largo no firmado

60 **Identificador de clase** Esta opción se especifica sólo en el cliente DHCP. El cliente genera esta información y no es necesario que se especifique. El tipo y la configuración del cliente, suministrados por éste al servidor. Por ejemplo, el identificador puede codificar la configuración de hardware específica de proveedor del cliente. Dicha información es una cadena de *n* octetos, que los servidores interpretan. Por ejemplo: hex: X' 01' X'02' X'03'. Los servidores no equipados para interpretar la información específica de clase enviada por un cliente deben ignorarla. La longitud mínima es 1 octeto.

Formato de la opción: D/N

61 **Identificador de cliente** Esta opción se puede especificar tanto en el cliente DHCP como en el servidor DHCP. El cliente DHCP puede utilizar la opción 61 para especificar el identificador exclusivo de cliente. El servidor DHCP puede utilizar la opción 61 para indexar la base de datos de enlaces de direcciones. Se espera que dicho valor sea exclusivo para todos los clientes de un dominio administrativo.

Formato de la opción: Cadena de caracteres

62 **Nombre de dominio NetWare/IP** Esta opción se especifica sólo en el servidor DHCP. El nombre del dominio Netware/IP. La longitud mínima es 1 octeto y la máxima 255

Formato de la opción: Cadena de caracteres

63 **NetWare/IP** Esta opción se especifica sólo en el servidor DHCP. Un código de opción con fines generales utilizado para transportar toda la información relacionada con NetWare/IP excepto el nombre del dominio NetWare/IP. Se transportará un cierto número de subopciones NetWare/IP mediante el código de opción. La longitud mínima es 1 y la máxima es 255.

Formato de la opción: Cadena de caracteres

64 **Nombre de dominio NIS** Esta opción se especifica sólo en el servidor DHCP. El nombre de dominio del cliente del servicio de información de red (NIS)+ V3. El dominio tiene el formato de una cadena de caracteres del juego de caracteres NVT ASCII. La longitud mínima es 1.

Formato de la opción: Cadena de caracteres

65 **Servidores NIS** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (en orden de preferencia) de los servidores de servicio de información de red (NIS)+ V3 disponibles para el cliente.

Formato de la opción: Direcciones IP

66 **Nombre del servidor** Esta opción se especifica sólo en el servidor DHCP. El nombre del servidor Trivial File Transfer Protocol (TFTP) utilizado cuando el campo “sname” de la cabecera DHCP se ha utilizado para opciones DHCP.

Formato de la opción: Cadena de caracteres

67 **Nombre del archivo de arranque** Esta opción se especifica sólo en el servidor DHCP. El nombre del archivo de arranque cuando el campo de archivo de la cabecera DHCP se ha utilizado para opciones DHCP. La longitud mínima es 1.

Nota: Utilice esta opción para pasar un nombre de archivo de arranque a un cliente DHCP. Es obligatorio que el nombre del archivo de arranque contenga el nombre de la vía de acceso totalmente calificada y que tenga menos de 128 caracteres. Por ejemplo: opción 67 c:\vía_acceso\nombre_archivo_arranque. Este archivo contiene información que se puede interpretar del mismo modo que el campo de extensión de proveedor de 64 octetos dentro de la respuesta BOOTP, con la excepción de que la longitud del archivo queda limitada por la cabecera BootP a 128 caracteres.

Formato de la opción: Cadena de caracteres

68 **Dirección de inicio** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (en orden de preferencia) de los agentes de inicio IP móviles disponibles para el cliente. Esta opción habilita un sistema principal móvil para derivar las direcciones de inicio móviles y determina la máscara de subred de la red de inicio. La longitud habitual es cuatro octetos, incluyendo sólo una dirección de inicio del agente de inicio, pero puede ser cero octetos. Una longitud cero indica que no hay disponible ningún agente de inicio.

Formato de la opción: Direcciones IP

69 **Servidores SMTP** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (en orden de preferencia) de los servidores de protocolo de transferencia de correo simple (SMTP) disponibles para el cliente.

Formato de la opción: Direcciones IP

70 **Servidor POP3** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (en orden de preferencia) de los servidores de protocolo de oficiona de correos (POP) disponibles para el cliente.

Formato de la opción: Direcciones IP

71 **Servidor NNTP** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (en orden de preferencia) de los servidores de protocolo de transferencia de noticias de red (NNTP) disponibles para el cliente.

Formato de la opción: Direcciones IP

72 **Servidor WWW** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (en orden de preferencia) de los servidores World Wide Web (WWW) disponibles para el cliente.

Formato de la opción: Direcciones IP

73 **Servidor Finger** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (en orden de preferencia) de los servidores Finger disponibles para el cliente.

Formato de la opción: Direcciones IP

74 **Servidor IRC** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (en orden de preferencia) de los servidores Internet Relay Chat (IRC) disponibles para el cliente.

Formato de la opción: Direcciones IP

75 **Servidor StreetTalk** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (en orden de preferencia) de los servidores StreetTalk disponibles para el cliente.

Formato de la opción: Direcciones IP

76 **Servidor STDA** Esta opción se especifica sólo en el servidor DHCP. Las direcciones IP (en orden de preferencia) de los servidores de asistencia de directorios StreetTalk (STDA) disponibles para el cliente.

Formato de la opción: Direcciones IP

77 **Clase de usuario** Esta opción se especifica sólo en el cliente DHCP. Los clientes DHCP utilizan la opción 77 para indicar a los servidores DHCP la clase de la que es miembro el sistema principal. Se puede entrar manualmente la clase de usuario en el archivo \DHCPCD.CFG como valor para la opción 77 a fin de recibir los parámetros definidos para dicha clase en un servidor DHCP. EL archivo DHCPCD.CFG está ubicado en el directorio ONDEMAND\SERVER\ETC.

Formato de la opción: Cadena de caracteres

78 **Agente de directorios** Esta opción se especifica sólo en el servidor DHCP. El protocolo de configuración dinámica de sistemas principales proporciona una infraestructura para pasar información de configuración a sistemas principales en una red TCP/IP. Es necesario que las entidades que utilizan el protocolo de ubicación de servicios conozcan las direcciones de los agentes de directorios a fin de tramitar mensajes. En algunas otras instancias, es probable que sea necesario que descubran el ámbito correcto y la autoridad de nombres que se deben utilizar junto con los atributos de servicio y URL que se intercambian mediante el protocolo de ubicación de servicios. Los agentes de directorios disponen de un ámbito particular y es probable que estén al corriente de los esquemas definidos por una autoridad de nombres concreta.

Formato de la opción: Dirección IP

79 **Ámbito del 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 tal y como especifica el protocolo de ubicación de servicios.

Formato de la opción: Cadena de caracteres

80 **Autoridad de nombres** Esta opción se especifica sólo en el servidor DHCP. Esta extensión indica una autoridad de nombres que especifica la sintaxis de los esquemas que se pueden utilizar en URL para que las entidades los utilicen, a su vez, con el protocolo de ubicación de servicios.

Formato de la opción: Cadena de caracteres

Opciones específicas de IBM

IBM proporciona un conjunto de sus opciones específicas definiendo las opciones del rango definido por el usuario (128-254). Tales opciones se utilizan sin que haya la necesidad de definir una opción de proveedor (opción 43) para IBM. Es recomendable que las vuelva a definir.

192 **TXT RR** Si se ha especificado esta opción en el servidor DHCP, es necesario que el usuario del cliente DHCP rellene los campos de información del administrador del sistema. Nota: Esta opción sólo recibe soporte en clientes TCP/IP Versión 4.1 para OS/2. Proporciona, además, hasta cuatro etiquetas de texto o campos de entrada obligatorios que el administrador del sistema puede especificar, entre los que se encuentran, por ejemplo, el nombre de un usuario, su número de teléfono u otros campos que el programa de configuración del cliente DDNS solicita a éste. Dichos campos permiten que el administrador del sistema identifique la persona real que ha configurado el nombre del 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 del DNS. Los pares de etiquetas de campos y datos son necesarios para ajustarse a un solo registro de recursos TXT. El espacio disponible se divide a partes iguales entre los pares. El valor se actualiza también en el archivo DDNSCLI.CFG del cliente de direcciones dinámicas.

Formato de la opción: Cadena de caracteres

Opciones de proveedor

El protocolo DHCP facilita un método para suministrar información específica de proveedor a un cliente DHCP mediante las opciones de la arquitectura RFC 43 y 60.

60 La **Opción 60** se configura en un cliente DHCP y se envía al servidor DHCP para identificar al primero como proveedor específico.

43 La **Opción 43** se configura en el servidor DHCP para definir la información específica de proveedor que debe volver al cliente en respuesta a la solicitud efectuada por el cliente mediante la opción 60. En lo que se refiere al servidor de código común DHCP, la opción se configura mediante el mandato add vendor-option. Las opciones de proveedor se definen únicamente dentro del 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 hex
Se entran con el nombre del proveedor cuando se ejecuta el mandato add vendor-option. Los datos hex se deben entrar como una cadena de caracteres hex con espacios en blanco entre los bytes: “01 AA 55”

Opciones

Se puede añadir cualquier opción DHCP a un ámbito de opción de proveedor mediante el mandato add option.

Nota: Los datos hex y las opciones se excluyen mutuamente en una definición de proveedor. Puede definir los unos o las otras pero no ambos.

Configuración de IP para DHCP

A fin de que el servidor DHCP asigne de manera satisfactoria direcciones IP e información de configuración para clientes de una subred añadida, es necesario que el IP esté configurado de manera adecuada. Ello se consigue cuando el servidor DHCP está conectado directamente a una subred que se ha configurado para ofrecer soporte.

Si se está utilizando un agente de BOOTP Relay para reenviar mensajes de peticiones DHCP a este servidor DHCP, es probable que no exista una configuración IP necesaria para dar soporte a una subred que no está conectada directamente al servidor.

Adición de una dirección IP

Es necesario que una dirección IP que se sitúe dentro de la subred configurada DHCP se añada a la interfaz de conexión. Si hay más de una dirección definida 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 procediera de la primera dirección que se ha encontrado para esa interfaz.

Nota: La primera dirección que se encuentra en una interfaz es la **última** dirección que se añade a la interfaz.

Ejemplo:

- DHCP ha añadido una subred de la forma 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 requerirá 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 del acceso simple a Internet del IP

Si el acceso simple a Internet se ha habilitado en IP y no se ha configurado previamente DHCP, se generará de manera automática en el servidor DHCP la siguiente configuración. El acceso simple a Internet también configurará de manera automática la función NAT y otros filtros y controles de acceso IP. Si DHCP ya está configurado, no se producirán cambios/adiciones en la configuración DHCP. Consulte Utilización del acceso simple a Internet en el capítulo "Utilización de IP" de la publicación *Configuración y supervisión de protocolos - Manual de consulta Volumen 1* si desea obtener más información general y sobre restricciones.

- Se ha configurado IP del siguiente modo:

```
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 generará 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 del servidor DHCP

Archivo de texto ASCII

Esta sección muestra una configuración de servidor DHCP habitual en formato de texto ASCII. Este ejemplo tiene únicamente el fin de ilustrar una configuración en

un formato que le puede ser familiar. El IBM 2212 no ofrece soporte a configuraciones ASCII.

Utilice los números bloqueados (**1**) como referencia para las funciones que se describen en este ejemplo de ASCII con la configuración `talk 6` equivalente que se describe en “Configuración de OPCON (talk 6)” en la página 503.

```
1  Configuration of Server parameters

leaseTimeDefault          120                 # 120 minutes
leaseExpireInterval       20 seconds
supportBOOTP              yes
supportUnlistedClients  yes


2  Global options.  Passed to every client unless overridden at a lower scope.

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  Vendor-options


vendor  XI-clients hex"01 02 03"

vendor XA-clients
{
   option 23 100   # IP TTL
}

4  A typical subnet

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  class manager defined at the subnet scope.  Option 9 here will override
the option 9 specified in the global manager class.
                 class manager

        {
                option 9   9.2.23.98
        }
```

```
6  Programmers have their own subnet range

        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  Example of a client that will accept any address but will have
its own set of options.

client 6        0x10005aa4b9ab  ANY
{
        option 51 999
        option 1 255.255.255.0
}

8  Exclude an address from service.

client 0       0              9.2.23.121
```

Configuración de OPCON (talk 6)

El siguiente es un ejemplo de la misma configuración utilizando esta vez `talk 6`.

```
| 1 Configuration of Server parameters

| 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 Global options.  Passed to every client unless overridden at a lower scope.

| 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
```

```
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 Vendor-options

```
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 A typical subnet

```
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 Programmers have their own subnet range

```
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
```

```
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 Example of a client that will accept any address but will have its own set of options.

```
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 Exclude an address from service.

```
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
```

Capítulo 31. Configuración y supervisión del servidor DHCP

Este capítulo describe cómo utilizar la configuración del servidor DHCP y sus mandatos operativos e incluye las siguientes secciones:

- "Acceso al entorno de configuración del servidor DHCP"
- "Mandatos de configuración del servidor DHCP"
- "Acceso al entorno de supervisión del servidor DHCP" en la página 541
- "Mandatos de supervisión del servidor DHCP" en la página 541

Acceso al entorno de configuración del servidor DHCP

Utilice el procedimiento siguiente 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>`) aparece en el terminal. Si el indicador no aparece cuando se entra por primera vez la configuración, pulse **Intro** de nuevo.

2. Entre el mandato **feature dhcp-server** en el indicador Config para acceder al indicador `DHCP Server config>`.

Mandatos de configuración del servidor DHCP

Tabla 58. Resumen de mandatos de configuración del servidor DHCP

Mandato	Función
? (Ayuda)	Visualiza todos los mandatos disponibles para este nivel de mandato, o lista las opciones de mandatos específicos (si es que están disponibles). Consulte "Obtención de ayuda" en la página xxv.
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 algunas variables globales a sus valores por omisión.
Delete	Suprime una clase, un cliente, una subred o una opción de proveedor.
Disable	Inhabilita globalmente el servidor DHCP.
Enable	Habilita globalmente el servidor DHCP.
List	Lista las definiciones de una clase, un cliente, globales, una subred o una opción de proveedor.
Set	Establece definiciones de parámetros u opciones globales de un ámbito especificado.
Exit	Hace volver al nivel de mandato anterior. Consulte "Salida de un entorno de nivel inferior" en la página xxv.

Add

Utilice el mandato **add** para añadir una clase, subred u opción de vendedor.

Sintaxis:

add class
client
option
subnet
vendor-option

clase *ámbito [nombre_subred] nombre_clase [inicio_rango] [fin_rango]*

Define una clase.

ámbito
Especifica el ámbito en el que se está añadiendo la clase.

Valores válidos: global o subnet

Valor por omisión: Ninguno

nombre_subred
Sólo es válida si el **ámbito** es *subnet*. Indica el nombre de la subred a la que se está añadiendo la clase.

Valores válidos: Cualquier nombre de subred existente

Valor por omisión: Ninguno

nombre_clase
Indica el nombre de la clase.

Valores válidos: Una cadena ASCII de hasta 40 caracteres

Valor por omisión: Ninguno

inicio_rango
Sólo es válida si el **ámbito** es *subnet*. Especifica la dirección IP de inicio de la agrupación de direcciones IP a la que se asignará el cliente.

Valores válidos: Cualquier dirección IP válida dentro del rango de la subred a la que se está añadiendo la clase.

Valores por omisión: La primera dirección IP del rango de subred que pertenece a la subred especificada.

fin_rango
Sólo es válida si el **ámbito** es *subnet*. Especifica la dirección IP final de la agrupación de direcciones IP a la que se asignará el cliente.

Valores válidos: Cualquier dirección IP válida dentro del rango de la subred a la que se está añadiendo la clase. Dicho valor debe ser mayor que el valor especificado para **inicio-rango**.

Valor por omisión: La dirección IP de inicio más 5 de las del rango de subredes que pertenece a la subred especificada. Si la dirección IP resultante no es mayor dentro del rango de subredes, el valor por omisión será la dirección IP final del rango de subredes.

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 está añadiendo el cliente.

Valores válidos: global o subnet

Valor por omisión: Ninguno

nombre-subred

Sólo es válida si el **ámbito** es *subnet* (subred). Indica el nombre de la subred a la que se está añadiendo el cliente.

Valores válidos: Cualquier nombre de subred existente

Valor por omisión: Ninguno

nombre-cliente

Indica el nombre del cliente.

Valores válidos: Cualquier cadena de caracteres ASCII de 10 caracteres

Valor por omisión: Ninguno

tipo-id

Indica el tipo de hardware del cliente. A continuación se muestran los tipos de hardware definidos en RFC 1340 que son aplicables al IBM 2212.

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 del cliente. Si el **tipo-id** es *0*, el **valor-id** debe ser una cadena de 64 caracteres. De lo contrario, el **valor-id** 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 o cualquier dirección MAC válida (12 dígitos hexadecimales)

Valor por omisión: Ninguno

dirección

Especifica la dirección IP a proporcionar al cliente o una cadena de caracteres que indica que el cliente no recibirá servicio o que se puede suministrar al cliente cualquier dirección de la agrupación de direcciones IP.

Valores válidos:

Cualquier dirección IP válida
En formato decimal por puntos. Si el cliente se define dentro de un ámbito de subred, la dirección IP debe formar parte de éste.

none Indica que el cliente coincidente no recibirá servicio

any Indica que se puede proporcionar al cliente cualquier dirección IP de la agrupación de subredes.

Valor por omisión: Ninguno

Nota: Un **tipo de id** de *0* y un **valor de 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 ser globales o encontrarse dentro de un ámbito de subred, clase, cliente u opción de vendedor.

ámbito

Especifica el ámbito al que se está añadiendo la opción.

Valores válidos:

- class-global
- class-subnet
- client-global
- client subnet
- global
- subnet
- vendor-option

Valor por omisión: Ninguno

nombre de subred
Sólo es válida si el **ámbito** es *subnet*, *class-subnet*, o *client-subnet*. Especifica el nombre de la subred a la que se está añadiendo el cliente.

Valores válidos: Cualquier nombre de subred existente

Valor por omisión: Ninguno

nombre de clase
Sólo es válida si el **ámbito** es *class-global* o *class-subnet*. Indica el nombre de la clase a la que se está añadiendo la opción.

Valores válidos: Un nombre de clase existente

Valor por omisión: Ninguno

nombre de cliente
Sólo es válida si el **ámbito** es *client-global* o *client-subnet*. Indica el nombre del cliente al que se está añadiendo la opción.

Valores válidos: Cualquier nombre de cliente existente

Valor por omisión: Ninguno

nombre de proveedor
Sólo es válida si el **ámbito** es *vendor-option*. Indica el nombre del proveedor al que se está añadiendo la opción.

Valores válidos: Cualquier nombre de proveedor existente

Valor por omisión: Ninguno

código Especifica el código de la opción. Las opciones DHCP se definen en RFC 2132. Consulte “Opciones DHCP” en la página 487 si desea obtener una descripción de las opciones y sus respectivos formatos.

Valores válidos: 1 - 255

Valor por omisión: 1

datos Especifica los datos de la opción. Los datos de la opción se pueden definir de tres maneras.

- Cadenas de caracteres ASCII para formatos específicos definidos en RFC 2132.
- Conversión hexadecimal en el momento de la inicialización. Los datos se deben entrar como *hex: 01 aa 04*.
- Cadena de caracteres. Los datos se deben entrar como *abcdef*.

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_subred] [prioridad_grupo_subred] [lista_política]*
Define una subred.

nombre de subred
Indica el nombre de la subred.

Valores válidos: Cualquier cadena de caracteres ASCII de 10 caracteres

Valor por omisión: Ninguno

dirección de subred
Especifica la dirección de la subred. La dirección se especifica en formato decimal por puntos.

Valores válidos: Cualquier dirección de subred IP válida.

Valor por omisión: Ninguno

máscara de subred
Especifica la máscara de la dirección de subred. La dirección de subred debe estar dentro de la máscara de subred y no puede contener un número mayor de bits que la máscara.

Valores válidos: Cualquier máscara IP válida en formato decimal por puntos

Valor por omisión: Se calcula en base a la dirección de subred

inicio de rango
Especifica la dirección IP de inicio de la agrupación de direcciones IP que el servidor administrará para esta subred. Si no se especifica *inicio_rango*, el servidor administra todas las direcciones de la subred.

Valores válidos: Cualquier dirección de sistema principal IP válida dentro de la subred especificada en formato decimal por puntos.

Valor por omisión: La primera dirección IP de la subred

fin de rango
Especifica la dirección IP final de la agrupación de direcciones IP que el servidor administrará para esta subred.

Valores válidos: Cualquier dirección de sistema principal IP válida dentro de la subred especificada en formato decimal por puntos.

Valor por omisión: inicio-rango más 50. Si la dirección IP resultante ya no se encuentra dentro de la subred, el valor por omisión será la última dirección IP de la subred.

nombre de grupo de subredes
Especifica el nombre del grupo de subredes al que pertenece la subred.

Valores válidos: Cualquier cadena ASCII de hasta 64 caracteres

Valor por omisión: Ninguno

prioridad de grupo de subredes
Especifica la prioridad de esta subred dentro del grupo de subredes. Esta prioridad se utiliza para determinar el orden en el que se asignan las direcciones dentro de un grupo de subredes específico.

Valores válidos: 1 - 65535

Valor por omisión: 1

lista de políticas
Identifica la lista de direcciones de política, Balance o Inorder, a la que se añadirá el grupo de subredes. Si el grupo de subredes ya existe en una de las listas y se especifica la otra, el grupo de subredes se moverá a la nueva lista.

Valores válidos: Inorder o Balance

Valor por omisión: Si se trata de una nueva subred, el valor por omisión es Inorder. De lo contrario, es la lista de política 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
```

opción de proveedor *nombre_proveedor [valor_hex]*

Añade una opción de proveedor. Existen dos maneras de proporcionar datos de opción de proveedor:

- Entrar datos hex cuando se solicita
- Añadir opciones específicas del proveedor mediante el mandato **add option vendor**. Consulte la página 512 si desea obtener información de opciones.

nombre_proveedor

Especifica el nombre del proveedor.

Valores válidos: Una cadena ASCII de hasta 40 caracteres

Valor por omisión: Ninguno

valor_hex

Especifica la cadena de caracteres ASCII hexadecimal que representa el valor hexadecimal de la parte destinada a datos de la opción.

Valores válidos: Cualquier cadena de caracteres hexadecimales válida en el siguiente formato: *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 está modificando.

Valores válidos: global o subnet

Valor por omisión: Ninguno

nombre de subred
Sólo es válida si el **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 de clase
Indica el nombre de la clase.

Valores válidos: El nombre de una clase existente

Valor por omisión: Ninguno

nuevo nombre de clase
Indica el nuevo nombre de la clase.

Valores válidos: Una cadena ASCII de hasta 40 caracteres

Valor por omisión: El nombre de la clase existente

nuevo inicio de rango
Sólo es válida si el **ámbito** es *subnet*. Especifica la nueva dirección IP de inicio de la agrupación de direcciones IP a la que se asignarán clientes.

Valores válidos: Cualquier dirección IP dentro del rango de subred

Valor por omisión: Inicio del rango existente

nuevo fin de rango
Especifica la nueva dirección IP final de la agrupación de direcciones IP a la que se asignarán clientes.

Valores válidos: Cualquier dirección IP válida dentro del rango de subredes y superior a **nuevo-fin-rango**

Valor por omisión: El rango existente

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_id_tipo nuevo_id_valor nueva_dirección*
Modifica un cliente

ámbito
Especifica el ámbito del cliente que se está modificando.

Valores válidos: global o subnet

Valor por omisión: Ninguno

nombre de subred
Sólo es válida si el **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 de cliente
Indica el nombre del cliente.

Valores válidos: Un nombre de cliente existente

Valor por omisión: Ninguno

nuevo nombre de cliente
Indica el nuevo nombre del cliente.

Valores válidos: Una cadena ASCII de hasta 10 caracteres

Valor por omisión: El nombre del cliente existente

nuevo tipo de id
Indica el nuevo tipo de hardware del cliente.

Valores válidos: 0 - 21. Consulte la página 511.

Valor por omisión: El tipo existente de hardware del cliente

nuevo valor de id
Especifica el nuevo identificador del cliente.

Valores válidos: 0 o cualquier dirección MAC válida (12 dígitos hexadecimales)

Valor por omisión: El tipo existente de id del cliente

Nota: Un **tipo-id** de *0* y un **valor-id** de *0* indican que el servidor no debe distribuir la dirección IP especificada.

nueva dirección
Especifica la nueva dirección IP a proporcionar al cliente o una cadena de caracteres que indica que el cliente no recibirá servicio o que se le puede proporcionar cualquier dirección de la agrupación de direcciones IP.

Valores válidos:

Cualquier dirección IP válida

none Indica que el cliente coincidente no recibirá servicio

any Indica que se puede proporcionar al cliente cualquier dirección IP de la agrupación de subredes.

Valor por omisión: Ninguno

Nota: Un **tipo de id** de *0* y un **valor de id** de *0* indican 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 de subred
Indica el nombre de la red específica a modificar.

Valores válidos: Un nombre de subred existente

Valor por omisión: Ninguno

nuevo nombre de subred
Indica el nuevo nombre de la subred especificada.

Valores válidos: Cualquier cadena de caracteres ASCII de 10 caracteres

Valor por omisión: El nombre de subred original

nueva dirección de subred
Especifica la nueva dirección de la subred. La dirección se especifica en notación decimal por puntos.

Valores válidos: Cualquier dirección de subred IP válida.

Valor por omisión: La dirección de subred existente

nueva máscara de subred
Especifica la nueva máscara de la dirección de subred. La dirección de subred debe estar dentro de la máscara de subred y no puede contener un número mayor de bits que la máscara.

Valores válidos: Cualquier máscara IP válida

Valor por omisión La máscara de subred existente

nuevo inicio de rango
Especifica la nueva dirección IP de inicio de la agrupación de direcciones IP que el servidor administrará para esta subred. Si no

se especifica *inicio-rango*, el servidor administra todas las direcciones de la subred.

Valores válidos: Cualquier dirección IP válida dentro del rango de subredes

Valor por omisión: La dirección de inicio de la agrupación existente

nuevo fin de rango
Especifica la nueva dirección IP final de la agrupación de direcciones IP que el servidor administrará para esta subred.

Valores válidos: Cualquier dirección IP válida dentro del rango de subredes y superior a la dirección de inicio de la agrupación.

Valor por omisión: La dirección final de la 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]?
```

opción de proveedor *nombre_proveedor nuevo_nombre_proveedor [nuevo_valor_hex]*
Modifica una opción de proveedor.

nombre de proveedor
Especifica el nuevo nombre de la opción de proveedor.

Valores válidos: Un nombre de proveedor existente

Valor por omisión: Ninguno

nuevo nombre de proveedor
Especifica el nuevo nombre de la opción de proveedor.

Valores válidos: Una cadena ASCII de hasta 40 caracteres

Valor por omisión: El nombre de la opción de proveedor existente

nuevo valor hex
Especifica la nueva cadena de caracteres ASCII hexadecimal que representa el valor hexadecimal de la parte destinada a datos de la opción. No se puede añadir un valor hex si se han añadido opciones específicas a esta opción de proveedor.

Valores válidos: Cualquier cadena de caracteres hexadecimales válida

Valor por omisión: La cadena de caracteres hexadecimales 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:

de**lete** class
client
option
subnet
subnet-group
vendor-option

class *ámbito [nombre_subred] nombre_clase*
Suprime una clase y todas las opciones definidas en su ámbito.

ámbito
Especifica el ámbito en el que se está suprimiendo la clase.

Valores válidos: global o subnet

Valor por omisión: Ninguno

nombre de subred
Sólo es válida si el **ámbito** es *subnet*. Especifica el nombre de la subred de donde se está suprimiendo la clase.

Valores válidos: Cualquier nombre de subred existente

Valor por omisión: Ninguno

nombre de clase
Indica el nombre de la clase a suprimir.

Valores válidos: Un nombre de clase existente

Valor por omisión: Ninguno

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 en su ámbito.

ámbito
Especifica el ámbito en el que se está suprimiendo el cliente.

Valores válidos: global o subnet

Valor por omisión: Ninguno

nombre de subred
Sólo es válida si el **ámbito** es *subnet*. Especifica el nombre de la subred de donde se está suprimiendo el cliente.

Valores válidos: Un nombre de subred existente

Valor por omisión: Ninguno

nombre de cliente
Indica el nombre del cliente 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 dentro del ámbito especificado.

ámbito
Especifica el ámbito en el que se está suprimiendo la opción.

Valores válidos:

- class-global
- class-subnet
- client-global
- client subnet
- global
- subnet
- vendor-option

Valor por omisión: Ninguno

nombre de subred
Sólo es válida si el **ámbito** es *subnet, class-subnet,* o *client-subnet*. Especifica el nombre de la subred de donde se está suprimiendo el cliente.

Valores válidos: Cualquier nombre de subred existente

Valor por omisión: Ninguno

nombre de clase
Sólo es válida si el **ámbito** es *class-global* o *class-subnet*. Indica el nombre de la clase de donde se está suprimiendo la opción.

Valores válidos: Un nombre de clase existente

Valor por omisión: Ninguno

nombre de cliente
Sólo es válida si el **ámbito** es *client-global* o *client-subnet*. Indica el nombre del cliente de donde se está suprimiendo la opción.

Valores válidos: Cualquier nombre de cliente existente

Valor por omisión: Ninguno

nombre de proveedor
Sólo es válida si el **ámbito** es *vendor-option*. Indica el nombre del proveedor de donde se está suprimiendo la opción.

Valores válidos: Cualquier nombre de proveedor existente

Valor por omisión: Ninguno

código Especifica el código de la opción. Las opciones DHCP se definen en RFC 2132. Consulte “Opciones DHCP” en la página 487 si desea obtener una descripción de las opciones y sus respectivos formatos.

Valores válidos: 1 - 255

Valor por omisión: 1

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 un subred y todas las clases, clientes y opciones que se definen en su ámbito.

nombre de subred

Especifica el nombre de la subred que se está suprimiendo.

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_subred*

Suprime todas las subredes asociadas con un grupo de subredes concreto y todas las clases, clientes y opciones definidas en los ámbitos de subred.

nombre de grupo de 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 todas las opciones definidas en su ámbito.

nombre de proveedor

Especifica el nombre del proveedor.

Valores válidos: Una cadena ASCII de hasta 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 el servidor DHCP globalmente.

Sintaxis:

disable dhcp-server

Ejemplo:

```
DHCP Server config> disable dhcp-server
```

Enable

Utilice el mandato **enable** para habilitar el servidor DHCP globalmente.

Sintaxis:

enable dhcp-server

Ejemplo:

```
DHCP Server config> enable dhcp-server
```

List

Utilice el mandato **list** para listar información de configuración sobre una clase, un cliente, parámetros globales, subredes u opciones de proveedor y sus opciones asociadas.

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.

class-name
Indica el nombre de la clase a visualizar.

Valores válidos: Un 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 todas las clases configuradas o los detalles de un cliente específico.

nombre de cliente

Indica el nombre del cliente a visualizar.

Valores válidos: Un nombre de cliente existente

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 los 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 está listando la opción.

Valores válidos:

- class-global
- class-subnet
- client-global
- client subnet
- global
- subnet
- vendor-option

Valor por omisión: Ninguno

nombre de subred
Sólo es válida si el **ámbito** es *subnet*, *class-subnet* o *client-subnet*. Especifica el nombre de la subred a la que pertenece la opción que se está listando.

Valores válidos: Cualquier nombre de subred existente

Valor por omisión: Ninguno

nombre de clase
Sólo es válida si el **ámbito** es *class-global* o *class-subnet*. Indica el nombre de la clase a la que pertenece la opción que se está listando.

Valores válidos: Un nombre de clase existente

Valor por omisión: Ninguno

nombre de cliente
Sólo es válida si el **ámbito** es *client-global* o *client-subnet*. Indica el nombre del cliente al que pertenece la opción que se está listando.

Valores válidos: Cualquier nombre de cliente existente

Valor por omisión: Ninguno

nombre de proveedor
Sólo es válida si el **ámbito** es *vendor-option*. Indica el nombre del proveedor al que pertenece la opción que se está listando.

Valores válidos: Cualquier nombre de proveedor existente

Valor por omisión: Ninguno

código Especifica el código de la opción. Las opciones DHCP se definen en RFC 2132. Consulte “Opciones DHCP” en la página 487 si desea obtener una descripción de las opciones y sus respectivos formatos.

Valores válidos: 1 - 255

Valor por omisión: 1

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 de subred

Indica el nombre de la subred a visualizar.

Valores válidos: Un nombre de subred existente

Valor por omisión: Ninguno

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    subnet     subnet        starting      ending
     name      address    mask          IP Addr       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     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

     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.

vendor-name

Indica el nombre de la opción de proveedor 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 los valores de los parámetros globales y para 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 modo rotatorio desde todas las subredes asociadas con los grupos definidos dentro de un grupo de subredes, en función de su prioridad.

nombre de grupo de 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
```

bootstrapserver *ámbito [nombre_subred] [nombre_clase] [nombre_cliente] dirección*
Indica si el servidor DHCP especifica o no un servidor bootstrap para clientes. Si desea que el servidor DHCP especifique un servidor bootstrap, deberá definir la dirección IP del servidor. Este parámetro se puede especificar dentro del ámbito global, de subred, de clase o de cliente.

ámbito
Especifica el ámbito del parámetro bootstrapserver.

Valores válidos:

- class-global
- class-subnet
- client-global
- client-subnet
- global
- subnet

Valor por omisión: Ninguno

nombre de subred
Sólo es válida si el ámbito es *subnet*, *class-subnet* o *client-subnet*. Indica el nombre de la subred para la que se está especificando el servidor bootstrap.

Valores válidos: Un nombre de subred existente

Valor por omisión: Ninguno

nombre de clase
Sólo es válida si el ámbito es *class-global* o *class-subnet*. Indica el nombre de la clase para la que se está especificando el servidor bootstrap.

Valores válidos: Un nombre de clase existente

Valor por omisión: Ninguno

nombre de cliente
Sólo es válida si el ámbito es *client-global* o *client-subnet*. Indica el nombre del cliente para el que se está especificando el servidor bootstrap.

Valores válidos: Un nombre de cliente existente

Valor por omisión: Ninguno

dirección IP del servidor
Especifica la dirección IP del servidor bootstrap.

Valores válidos: Cualquier dirección IP válida en formato decimal por 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 direcciones MAC en direcciones de formato canónico.

Las direcciones MAC de los clientes Ethernet/802.3 se almacenan en formato canónico (el byte empieza con el bit menos significativo). Las direcciones MAC para clientes Token-Ring se almacenan en el formato no canónico (el byte empieza con el bit más significativo). Este parámetro se debe utilizar cuando el servidor DHCP se encuentra en un tipo de medio (Token-Ring o Ethernet/802.3), el cliente en otro tipo de medio y existe un puente de conversión entre ambos. Cuando este parámetro se establece en *yes* (sí), el servidor DHCP hará que la dirección MAC del cliente se transforme de canónica a no canónica o, al contrario, de no canónica a canónica. Puesto que el servidor DHCP no conoce el formato en el que estaba originalmente la dirección MAC, al establecer este parámetro en *yes* (sí) la dirección cambiará simplemente de una a otra. Una dirección canónica se puede establecer dentro del ámbito global, de subred, de clase o de cliente.

ámbito
Especifica el ámbito del parámetro bootstrapserver.

Valores válidos:

- class-global
- class-subnet
- client-global
- client-subnet

- global
- subnet

Valor por omisión: Ninguno

nombre de subred
Sólo es válida si el ámbito es *subnet*, *class-subnet* o *client-subnet*. Indica el nombre de la subred para la que se está especificando la dirección canónica.

Valores válidos: Un nombre de subred existente

Valor por omisión: Ninguno

nombre de clase
Sólo es válida si el ámbito es *class-global* o *class-subnet*. Indica el nombre de la clase para la que se está especificando la dirección canónica.

Valores válidos: Un nombre de clase existente

Valor por omisión: Ninguno

nombre de cliente
Sólo es válida si el ámbito es *client-global* o *client-subnet*. Indica el nombre del cliente para el que se está especificando la dirección canónica.

Valores válidos: Un nombre de cliente existente

Valor por omisión: Ninguno

valor Especifica si las direcciones MAC se deben transformar a formato canónico

Valores válidos: yes (sí), no

Valor por omisión: no, si el **ámbito** es *global*. De lo contrario, el valor por omisión se determina mediante la jerarquía de ámbitos. Consulte “Conceptos y terminología” en la página 484 se desea obtener una descripción del concepto ámbito.

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 dicha subred.

nombre de grupo de 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 duración*

Especifica el intervalo al cabo del cual se examina la condición de cesión de todas las direcciones de la agrupación de direcciones para determinar las cesiones que han caducado. El intervalo de caducidad de la cesión sólo se puede establecer a nivel global.

tiempo

Especifica la unidad de medida de tiempo.

Valores válidos: segundos, minutos, horas

Valor por omisión: Ninguno

duración
Especifica la duración 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 duración*
Especifica la duración de la cesión por omisión para las cesiones ejecutadas por el servidor DHCP. Un intervalo infinito significa que las cesiones nunca caducarán. El valor por omisión del tiempo de cesión sólo se puede establecer a nivel global.

tiempo
Especifica la unidad de medida de tiempo.

Valores válidos: minutos, horas, días, semanas, meses, años, infinito

Valor por omisión: Ninguno

duración
Especifica la duración 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)

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 duración*

Antes de asignar una dirección IP, el servidor DHCP efectúa una prueba para asegurarse de que la dirección IP no está en uso. Este valor especifica el intervalo durante el que el servidor DHCP esperará una respuesta ping antes de marcar la dirección disponible. Un valor de 0 inhabilita los pings, lo que hace que el servidor DHCP no pruebe una dirección antes de asignarla.

tiempo

Especifica la unidad de medida de tiempo.

Valores válidos: segundos

Valor por omisión: Ninguno

duración

Especifica la duración 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 peticiones de clientes BOOTP. Si el servidor DHCP no se ha configurado previamente para ofrecer soporte a clientes BOOTP y se ha reconfigurado para no ofrecer soporte a clientes

BOOTP, el enlace de direcciones de los clientes BOOTP que se haya establecido antes de la reconfiguración se mantendrá hasta que el cliente BOOTP envíe otra petición (cuando se está iniciando). En ese momento, el servidor no responderá y se eliminará el enlace. Este parámetro sólo se puede establecer a nivel global.

Valores válidos: yes (sí) 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 que no sean aquéllos cuyos ID se listan de manera específica en esta configuración. Este parámetro dispone de 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 de subred

Sólo es válida si el ámbito es *subnet*, *class-subnet* o *client-subnet*. Indica el nombre de la subred para la que se está especificando este parámetro.

Valores válidos: Un nombre de subred existente

Valor por omisión: Ninguno

nombre de clase

Sólo es válida si el ámbito es *class-global* o *class-subnet*. Indica el nombre de la clase para la que se está especificando este parámetro.

Valores válidos: Un nombre de clase existente

Valor por omisión: Ninguno

valor

yes El servidor DHCP debe responder a cualquier cliente sin tener en cuenta el tipo al que pertenece o si está configurado.

no El servidor DHCP responderá sólo a las peticiones de clientes DHCP que estén configurados.

bootp El servidor DHCP ofrecerá soporte a clientes BOOTP no listados pero no lo ofrecerá a clientes DHCP no listados.

dhcp El servidor DHCP responderá a clientes DHCP no listados pero no lo hará a clientes BOOTP no listados.

Valores válidos: yes (sí), no, bootp, dhcp

Valor por omisión: yes (sÍ), si el **ámbito** es *global*. De lo contrario, el valor por omisión se determina mediante la jerarquía de ámbitos. Consulte “Conceptos y terminología” en la página 484 se desea obtener una descripción del concepto 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 duración*

Especifica el intervalo durante el que el servidor mantendrá una dirección IP en uso antes de ponerla a disposición para su asignación. Antes de que el servidor asigne una dirección IP, éste ejecuta ping en la dirección para asegurarse de que no se está utilizando ya en la red. Si es así, marca la dirección en uso como reservada. Este parámetro especifica el intervalo durante el que se mantiene como reservada una dirección en uso antes de ponerla a disposición para su asignación. Este parámetro sólo se puede establecer a nivel global.

tiempo

Especifica la unidad de medida de tiempo.

Valores válidos: segundos, minutos, horas, días, semanas, meses, años, infinito

Valor por omisión: Ninguno

duración

Especifica la duración 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 del servidor DHCP

Utilice el procedimiento siguiente para acceder al proceso de *supervisión* del servidor DHCP.

1. Entre **talk 5** en el indicador OPCON. Por ejemplo:

   ```
   * talk 5
   Config>
   ```

   Después de entrar el mandato **talk 5**, el indicador CONFIG (+) aparece en el terminal. Si el indicador no aparece cuando se entra por primera vez la configuración, pulse **Intro** de nuevo.
2. En el indicador +, entre el mandato **feature dhcp-server** para acceder al indicador DHCP Server>.

Mandatos de supervisión del servidor DHCP

Tabla 59 (Página 1 de 2). Resumen de mandatos de supervisión del servidor DHCP

Mandato	Función
? (Ayuda)	Visualiza todos los mandatos disponibles para este nivel de mandato, o lista las opciones de mandatos específicos (si es que están disponibles). Consulte “Obtención de ayuda” en la página xxv.

Tabla 59 (Página 2 de 2). Resumen de mandatos de supervisión del servidor DHCP

Mandato	Función
Disable	Inhabilita dinámicamente el servidor DHCP.
Enable	Habilita dinámicamente el servidor DHCP.
List	Visualiza los parámetros de clases, de clientes, globales, de subredes y de opciones de proveedor.
Reset	Restablece dinámicamente la configuración del servidor DHCP.
Request	
Exit	Hace volver al nivel de mandato anterior. Consulte “Salida de un entorno de nivel inferior” en la página xxv.

Disable

Utilice el mandato **disable** para inhabilitar de manera dinámica al 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 de una clase, un cliente, de parámetros globales, de subredes o de una opción de proveedor y sus opciones asociadas. Consulte “List” en la página 525 para obtener ejemplos del mandato **list**.

Sintaxis:

list	class
	client
	global
	option
	subnet
	vendor-option

Reset

Utilice el mandato **reset** para restablecer de manera dinámica 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 información de administración.

Sintaxis:

request clientid
delete
ipquery
poolquery
stats
status

clientid *id_cliente*

Visualiza información de un cliente.

client_id

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 una cesión de una dirección específica IP del cliente.

dirección

Indica la dirección IP del cliente que se debe 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 *dirección*

Visualiza información de una dirección IP.

Ejemplo:

Mandatos de supervisión del servidor DHCP (talk 6)

```
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 de una agrupación de direcciones IP.

dirección

Indica una dirección IP de la agrupación a visualizar.

Valores válidos: Cualquier dirección IP válida de la agrupación 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 sobre la agrupación de direcciones administradas por el servidor. Dichas estadísticas incluyen: los paquetes de descubrimiento procesados, los paquetes de descubrimiento sin respuesta, las ofertas efectuadas, las cesiones concedidas, los reconocimientos negativos (NAK), los informes procesados (incluyendo los informes más los reconocimientos, ACK), las renovaciones, las entregas, los clientes BOOTP procesados, los proxyARec actualizados intentados y los paquetes sin soporte. Sintaxis: request stats

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 sobre 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
```

Mandatos de supervisión del servidor DHCP (talk 6)

Capítulo 32. Utilización de la Thin Server Feature

En este capítulo se describe el modo de utilización de la Thin Server Feature (TSF) en el IBM 2212.

Visión general de la Network Station

Una Network Station es similar a un PC ya que dispone de un teclado, una pantalla y un ratón. La principal diferencia entre una Network Station y un PC es que los archivos de la Network Station residen en un servidor de red en lugar de en una unidad de disco duro de la máquina. La Network Station dispone de una interfaz gráfica de usuario (GUI), que proporciona acceso a muchos recursos, incluidos emuladores, aplicaciones X remotas, navegadores de Web, aplicaciones e impresoras.

La Network Station se comunica mediante TCP/IP a través de una conexión de red en anillo o Ethernet con el servidor. El proceso de encendido de la Network Station es el que sigue:

- Se inicia un programa supervisor de arranque residente en la memoria de acceso aleatorio no volátil y se ejecutan autopruebas de encendido.
- La Network Station contacta con un servidor BootP o DHCP que proporciona a la Network Station información tal como su dirección IP, las direcciones de servidor y la vía de acceso y el nombre del archivo de arranque. Como alternativa, la Network Station puede recuperar esta información a partir de los valores almacenados en su memoria de acceso aleatorio no volátil.
- La Network Station utiliza el protocolo de transferencia de archivos trivial (TFTP), el sistema de archivos remoto/400 (RFS/400) o el sistema de archivos de red (NFS) para bajar del servidor de código base el código base, como puede ser el sistema operativo, los archivos de configuración de hardware y los programas de aplicaciones.
- La Network Station baja del servidor de configuración del terminal la información de configuración basada en el terminal, como puede ser la configuración de una impresora conectada a la Network Station o el idioma del teclado de la Network Station.
- La Network Station muestra una pantalla de inicio de sesión. En ese momento, puede entrar un id de usuario y una contraseña.
- El servidor de autenticación valida el id de usuario y la contraseña y permite acceder a los archivos de usuario personales.
- Se bajan las preferencias de entorno del usuario.
- La Network Station visualiza el escritorio personalizado del usuario.

Consulte la publicación *IBM Network Station Manager Instalación y utilización*, SC10-3261 (SC41-0664), si desea más información sobre Network Stations.

Visión general de la Thin Server Feature

Un dispositivo físico puede funcionar como servidor BootP/DHCP, servidor de arranque, servidor de configuración del terminal y servidor de autenticación o cada uno de estos servidores puede ser un dispositivo independiente. Por ejemplo, puede disponer de una Network Station conectada a un AS/400 y que el AS/400

funcione como servidor BootP, servidor de código base, servidor de configuración del terminal y servidor de autenticación. Como alternativa, cada servidor puede ser una caja física independiente. 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 del terminal y otro AS/400 es su servidor de autenticación.

La Thin Server Feature permite que el 2212 se convierta en servidor de código base. Un ejemplo de por qué sería deseable utilizar la TSF queda ilustrado en la Figura 47 en la página 549 y la Figura 48 en la página 549. En la Figura 47 en la página 549, cualquier archivo que la Network Station necesite se bajará de un único servidor. Cuando se enciende la Network Station, la bajada supone la utilización de bastantes megabytes. Ello puede suponer una notable exigencia para una infraestructura de red, así como también para un dispositivo que actúe de servidor de código base/configuración de terminal o como servidor de autenticación, especialmente si hay muchas Network Stations encendidas. La Figura 48 en la página 549 muestra la red con un Thin Server utilizado en el sitio remoto. El Thin Server guardará en la antememoria muchos de los archivos asociados con el código de arranque de la Network Station. Cuando se enciende la Network Station, la mayor parte del código de arranque se cargará a partir del Thin Server y sólo será necesario que una pequeña cantidad de datos sea transportada por la infraestructura de la red. Este proceso reducido en cualquier servidor individual disminuye el tráfico de red y reduce el tiempo necesario para completar el encendido de una Network Station.

Como los archivos guardados en la antememoria por el Thin Server son copias de los archivos que residen en el servidor de archivos maestro, a medida que la versión del servidor de archivos maestro se modifica, es necesario que el Thin Server actualice su versión de este archivo. El Thin Server verificará que todos los archivos guardados en la antememoria sean idénticos a la versión del servidor de archivos maestro de aquellos archivos cuando:

1. Se enciende el IBM 2212
2. Se vuelve a cargar o se reinicia el IBM 2212
3. Se reinicia la TSF
4. Se alcanza el intervalo de tiempo especificado en la configuración de la TSF
5. Un parámetro de MIB SNMP lo desencadena
6. Se ejecuta el mandato `talk 5` **refresh** de la TSF
7. Siempre que se accede a un archivo (excepto TFTP). La TSF verificará que cada archivo al que se accede coincida con la versión del servidor de archivos maestro. Cuando se detecte una diferencia, dicho archivo se actualizará. A continuación, la TSF verificará que los archivos restantes coincidan también con el servidor de archivos maestro.

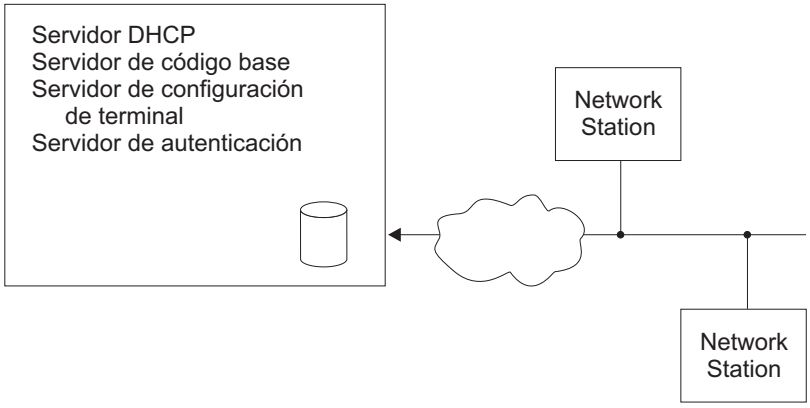


Figura 47. Estación de red remota sin Thin Server

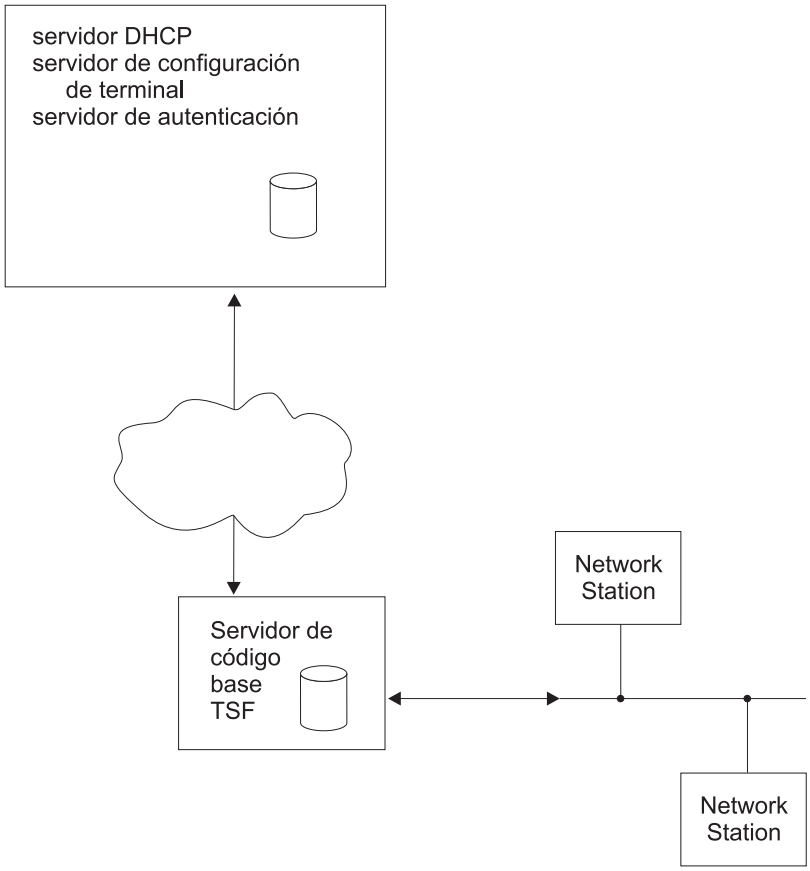


Figura 48. Estación de red remota con un Thin Server

Soporte de BootP/DHCP

Existen dos opciones de soporte para servidores BootP/DHCP:

- Utilizar el soporte del servidor DHCP del IBM 2212. Consulte Capítulo 30, "Utilización del Servidor DHCP" en la página 479.
- Configurar el IBM 2212 para que funcione como agente de retransmisión para las peticiones BootP/DHCP. Consulte el *Configuración y supervisión de protocolos - Manual de consulta Volumen 1* si desea obtener más información.

Consulte la publicación *IBM Network Station Manager Instalación y utilización*, SC10-3261 (SC41-0664), si desea más información sobre entornos multiservidor.

Protocolos utilizados para comunicar con Network Stations

Los protocolos que se utilizan para establecer comunicación entre la Network Station y sus servidores están determinados por la configuración BootP/DHCP o la configuración NVRAM de la Network Station. En cualquiera de los dos casos, los protocolos que la Network Station utiliza deben ser compatibles con la configuración de la TSF.

Si la TSF está configurada para utilizar RFS para comunicar con el servidor de archivos maestro, aceptará las peticiones RFS y TFTP de las Network Stations y no responderá a ninguna petición NFS de las Network Stations.

De manera similar, si la TSF está configurada para utilizar NFS para comunicar con el servidor de archivos maestro, aceptará las peticiones NFS y TFTP de las Network Stations y no responderá a ninguna petición RFS de las Network Stations.

Utilización de RFS

La TSF establece una conexión con el AS/400 mediante RFS. Cuando una Network Station efectúa una petición para abrir un archivo, la TSF reenvía esa petición al AS/400 para su autorización. Si la Network Station no está autorizada, la 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 la TSF del IBM 2212, la petición de la Network Station se retransmite al AS/400. Si el archivo de AS/400 tiene la misma versión que el archivo que la TSF ha guardado en antememoria, la TSF servirá dicho archivo a la Network Station.

Si la conexión TSF con el AS/400 no está disponible, la TSF servirá los archivos que ha guardado actualmente en antememoria en la Network Station.

Utilización de TFTP

Si se utiliza TFTP para comunicar entre la Network Station y la TSF, la TSF atenderá las peticiones de archivos de la Network Station si dichos archivos están disponibles. No se efectúa ninguna verificación de versión entre la TSF y el servidor de archivos maestro. Si el archivo no está disponible en la antememoria de la TSF, la petición de la Network Station se reenvía al servidor de archivos maestro.

Utilización de NFS

Si se utiliza NSF para comunicar entre la Network Station y la TSF, cuando una Network Station solicita un archivo, la TSF empezará a servir dicho archivo si se encuentra en la antememoria. De manera simultánea, verificará que el archivo tengar la misma versión que el servidor de archivos maestro. Si no es así, la TSF dejará de servir el archivo e iniciará de inmediato la bajada de la nueva versión del servidor de archivos maestro.

Si la TSF no tiene el archivo en antememoria, la TSF devolverá un mensaje de "archivo no encontrado". Así mismo, si el archivo solicitado reside en un directorio para el que se ha configurado la TSF con *include subdirectories* o reside en un

subdirectorio de dicho directorio configurado, la TSF empezará a guardar en antememoria el archivo, si el archivo existe en el servidor de archivos maestro.

Actualizaciones de antememorias de archivos

El protocolo utilizado para guardar un archivo en la antememoria en el IBM 2212 queda determinado por la configuración de la TSF. Los servidores maestros se designan mediante el mandato **add master-file-server**.

Si especifica *rfs*, se le solicitará que suministre un nombre de archivo de lista de precarga. La lista de precarga es un archivo ASCII que especifica el nombre de archivo totalmente cualificado de cada archivo que la TSF debe guardar en antememoria.

Si especifica *nfs*, se le solicitarán los nombres de los directorios que se deben guardar en antememoria (puede que se proporcionen algunos valores por omisión). Cuando especifique un directorio, se le solicitará si desea incluir o no subdirectorios. Si especifica *no* (no incluir subdirectorios), la TSF precargará todos los archivos en el directorio especificado de la antememoria de la TSF. Si especifica *yes* (incluir subdirectorios), la TSF NO precargará ningún archivo de ese directorio, sino que recuperará de manera dinámica archivos de dicho directorio y de cualquiera de sus subdirectorios a medida que las Network Stations soliciten dichos archivos.

Los archivos que se encuentran en proceso de renovación no se enviarán a la Network Station durante este proceso.

Configuración del entorno del Thin Server

Cuando la TSF está instalada, existen varias configuraciones además de la configuración de la propia TSF que se deben tener en cuenta. Esta sección comenta los cambios que puede que sean necesarios para la configuración del servidor BootP/DHCP, del servidor de archivos maestro, del IBM 2212 BootP Relay, de la dirección IP interna del IBM 2212 y de la TSF del IBM 2212. Encontrará un ejemplo de un Thin Server en conexión con un AS/400 que ejecuta el Network Station Manager Release 2.5 en “Ejemplo de configuración” en la página 553.

Las siguientes secciones describen el proceso de configuración del entorno Thin Server:

- “Recomendaciones de configuración”
- “Configuración del servidor BootP/DHCP” en la página 552
- “Configuración del servidor para el entorno del Thin Server” en la página 553
- “Configuración de BootP Relay” en la página 553
- “Configuración de la dirección IP interna” en la página 553
- “Configuración de la TSF” en la página 553
- “Ejemplo de configuración” en la página 553

Recomendaciones de configuración

A continuación encontrará algunas recomendaciones de configuración que le ayudarán a sacar el máximo partido al TSF:

- Utilizar un disco fijo.

Aunque la TSF no requiere un disco fijo, éste mejorará el rendimiento si la antememoria de la TSF se ha configurado en un valor demasiado bajo (o no se puede configurar lo suficientemente grande a causa de otras funciones del 2212) y también mejorará el rendimiento si la TSF o el 2212 se reinicia o se vuelve a cargar.

- Número máximo de Network Stations.

  La TSF permitirá hasta 200 conexiones de Network Stations RFS a la vez. Encender de manera simultánea más de 30 a 40 Network Stations puede ocasionar retrasos que hagan superar los valores de tiempo de espera de la Network Station. Puede que sea necesario volver a encender la Network Station para la recuperación.
- El servidor de archivos maestro debe ser un servidor que ejecute Network Station Manager.

  Aunque la TSF permite que la dirección IP del servidor de archivos maestro sea 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 la TSF y pueda proporcionar los archivos que la TSF solicitará.
- Definir suficiente memoria para contener todos los archivos guardados en antememoria.

  Esto es necesario si no se dispone de un disco fijo. Si no dispone de un disco fijo, el acceso a la memoria es mucho más rápido que el acceso al disco fijo. La cantidad de memoria necesaria variará en función del entorno específico. Utilice el mandato `Talk 5` **list config** para determinar el tamaño del conjunto de archivos en un momento determinado. El valor que se visualiza en *Hard File storage being used for Thin Server* es el tamaño del conjunto de archivos en kilobytes. De todos modos, si se añaden diferentes tipos de Network Stations al entorno o se eliminan de él, este valor puede cambiar.
- Si está utilizando NFS, la TSF averígua qué archivos que necesita.

  Este proceso de averiguación puede necesitar varias secuencias de encendido de la Network Station para que el TFS identifique todos los archivos necesarios.

Configuración del servidor BootP/DHCP

Cuando se ejecuta el Network Station Manager Release 3, DHCP es obligatorio si se está utilizando un Thin Server. Si está utilizando un AS/400 como servidor de archivos maestro, se puede utilizar el Network Station Manager Release 2.5, en cuyo caso se puede utilizar BootP en lugar de DHCP.

En el caso de BootP, sólo se puede especificar una dirección de servidor. Dicha dirección se especifica mediante el identificador **sa**. Puede que dicho identificador exista o no en el registro BootP de una Network Station determinada. Si no existe, créelo y establezca el valor en la dirección IP interna del 2212. Si existe ya, cámbielo por la dirección IP interna del 2212.

En el caso de DHCP, es probable que sea necesario modificar los campos cuando el Thin Server se utiliza del modo siguiente:

- Opción 66 o servidor bootstrap - dirección IP del servidor de código base

  Este valor se debe establecer en la dirección IP interna del IBM 2212
- Opción 211 - protocolo a utilizar para el servidor de código base

Si el Thin Server se está configurando para NFS de tipo servidor de archivos maestro, debe ser *nfs* o *tftp*. Si el Thin Server se está configurando para RFS de tipo 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. NO DEBE ser la dirección IP del Thin Server.

Si desea obtener más detalles acerca de cómo las NS interactúan con BootP y DHCP, consulte la publicación *IBM Network Station Manager Instalación y utilización*, SC10-3261 (SC41-0664).

Configuración del servidor para el entorno del Thin Server

En el caso de RFS, la lista de precarga debe estar instalada en el AS/400. La lista de precarga está disponible en la dirección de internet `http://www.networking.ibm.com/netprod.html#routers`. Debe ejecutar ftp para el archivo LoadList.file desde dicho sitio y ubicarlo en `/QIBM/ProdData/OS400/NetStationRmtController` del AS/400. Puede que sea necesario crear el directorio NetStationRmtController.

En el caso de NFS, no se necesita ningún cambio especial para el Thin Server.

Configuración de BootP Relay

Se debe habilitar el agente BootP Relay del IBM 2212 y se deben configurar los servidores BootP y DHCP para que el BootP Relay reenvíe a dichos servidores. Consulte la publicación *Software de Access Integration Services Guía del usuario* si desea obtener más información.

Configuración de la dirección IP interna

Si ya existe una dirección IP interna, no es necesario ningún cambio especial. Si hay ninguna dirección IP interna especificada actualmente, se deberá especificar una. Consulte la publicación *Configuración y supervisión de protocolos - Manual de consulta Volumen 1* si desea obtener más información.

Configuración de la TSF

Utilice los mandatos descritos en el Capítulo 33, “Configuración y supervisión de la Thin Server Function” en la página 559 para configurar el Thin Server.

Como mínimo, se deben entrar los siguientes mandatos:

1. **load add package thin-server**
2. **set mode enable**
3. **add master-server**

Ejemplo de configuración

El siguiente ejemplo muestra cómo configurar una TSF destinada a un AS/400 en el que se ejecuta Network Station Manager R2.5.

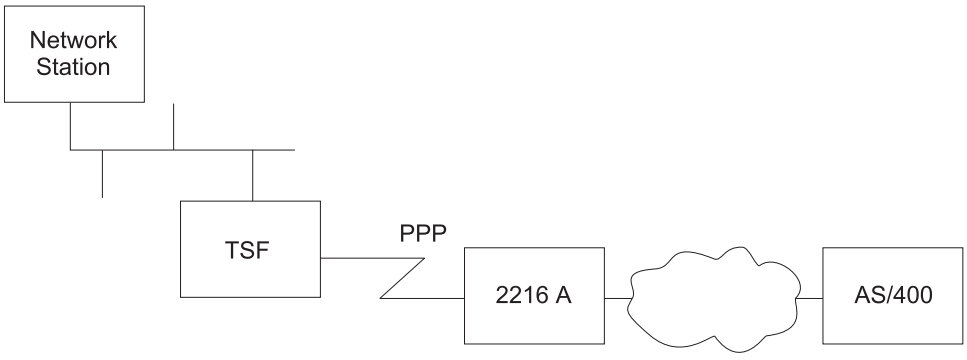


Figura 49. Ejemplo de configuración de la TSF

Esta descripción de la configuración de Thin Server Feature está basada en la red anterior y utiliza los siguientes supuestos:

- El AS/400 será el servidor BootP.
- El 2216 A es un direccionador (sin ningúna TSF configurada ni ninguna configuración especial para la TSF).
- La conectividad IP de la red se ha validado, es decir, el AS/400 puede ejecutar PING en el IBM 2212 (TSF) y el IBM 2212 puede ejecutar PING en el AS/400.
- BootP Relay NO está habilitado en la actualidad en el IBM 2212 (TSF)
- No hay configurada una dirección IP interna en el IBM 2212 (TSF)

Configuración del AS/400

BootP (NSM Release 2.5)

1. Utilice NSM para definir la NS
2. Ejecute ftp para transferir la tabla BootP a un sistema que disponga de 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 mediante un editor ASCII, añadiendo un identificador "sa" con la dirección IP interna del 2212 (TSF).

```
LÍNEA ANTIGUA
-------------
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

LINEA MODIFICADA
----------------
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 transferir la tabla BootP otra vez 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
```

Preparación de la lista de precarga

Puede obtener una lista de precarga de internet:
http://www.networking.ibm.com/netprod.html#routers

Una vez disponga de la lista de precarga, puede ejecutar ftp para transferirla al AS/400.

1. Asegúrese de que el directorio local se ha establecido en la ubicación del archivo "LoadList.file".
2. Ejecute ftp hacia el 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 del 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, deberá 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 TCP/IP dependerá del entorno específico.

Configuración del IBM 2212 (TSF)

BootP Relay

1. Determine si el 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 todavía no está habilitado, 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 Stations no está en la lista de 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 las direcciones de nuevo.

```
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>
```

Thin Server Feature

1. Añada el paquete de carga del Thin Server.

   Para poder configurar la Thin Server Feature, debe añadir el paquete de carga.

   En primer lugar, asegúrese de que el paquete del Thin Server está disponible.

   ```
   Config>load list available Available Packages
   ------------------
   appn package
   tn3270e package
   thin-server package
   Config>
   ```

   Si no está disponible, es necesario que obtenga la versión de software correcta antes de continuar.

   Si está disponible, verifique que el paquete no se haya cargado ya.

   ```
   Config>load list configured
   Configured Packages
   ------------------
   thin-server package
   Config>
   ```

   Si ya está cargado/configurado (como muestra el ejemplo anterior), puede continuar con la configuración de la TSF. Si todavía no se ha cargado, deberá añadir el paquete del Thin Server:

   ```
   Config>load add package thin-server
   thin-server package configured successfully
   This change requires a reload.
   Config>
   ```

2. Vuelva a cargar

   Si ha tenido que añadir el paquete del Thin Server, deberá escribir ahora la configuración y volver a cargar el IBM 2212.

3. Establezca la modalidad habilitada

   Cuando se carga el paquete, Thin Server está inicialmente inhabilitado. La modalidad se debe establecer como habilitada para poder configurar cualquier otro parámetro del 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. Añada un servidor de archivos maestro.

   Una vez que se ha habilitado la Thin Server Feature, se debe configurar el servidor de archivos maestro. En ese caso, el servidor de archivos maestro es un AS/400, de manera que añadiremos un servidor de archivos maestro RFS. En el caso de esta red, los parámetros de reintento y tiempo de espera TFTP por omisión son los 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 del AS/400 en la interfaz de red en anillo es 9.37.100.68. Cuando hemos instalado el archivo de lista de precarga en el AS/400 hemos asignado su nombre para que coincida con el nombre por omisión del Thin Server a fin de que no tenga que ser modificado.

5. Establezca la hora de renovación de la lista de precarga (opcional)

   El valor por omisión de la hora del día para llevar a cabo la renovación es la 1:00 AM. Se eligió esta hora para minimizar cualquier impacto de rendimiento si se han modificado archivos grandes y el Thin Server debe bajarlos.

6. Establezca el intervalo de la lista de precarga (opcional)

   El intervalo por omisión para verificar que los archivos guardados en la antememoria están al mismo nivel que el servidor de archivos maestro es cada día. El valor de este parámetro y el parámetro de hora de renovación de la lista de precarga determinan la frecuencia con la que se verifican los archivos. Si los archivos de la Network Station cambian de manera poco frecuente, es posible que desee que éstos sólo se renueven una vez a la semana o una vez al mes.

7. Establezca la memoria (opcional).

   La memoria por omisión de una antememoria RAM de 16 MB para guardar archivos debe ser suficiente. Una vez que varias Network Stations estén utilizando la TSF, consulte “Recomendaciones de configuración” en la página 551 para obtener los valores recomendados.

8. Establezca el disco fijo (opcional)

   Se recomienda un disco fijo. Si no dispone de un disco fijo, este parámetro se debe establecer en *no*.

Capítulo 33. Configuración y supervisión de la Thin Server Function

Este capítulo describe cómo utilizar los mandatos de configuración y operación de la Thin Server Function (TSF) y consta de las siguientes secciones:

- "Acceso al entorno de configuración de la TSF"
- "Mandatos de configuración de la TSF"
- "Acceso al entorno de supervisión de la TSF" en la página 569
- "Mandatos de supervisión de la TSF" en la página 569

Acceso al entorno de configuración de la TSF

Utilice el procedimiento siguiente para acceder al proceso de configuración de la TSF.

1. En el indicador OPCON, entre **talk 6**. (Si desea obtener más detalles sobre este mandato, consulte "The OPCON Process and Commands" en la publicación *Software de Access Integration Services Guía del usuario*.) Por ejemplo:

   ```
   * talk 6
   Config>
   ```

   Después de entrar el mandato **talk 6**, el indicador CONFIG (`Config>`) aparece en el terminal. Si el indicador no aparece cuando se entra por primera vez en la configuración, pulse **Intro** de nuevo.
2. Entre el mandato **feature tsf** en el indicador CONFIG para acceder al indicador `Thin server config>`.

Mandatos de configuración de la TSF

Para configurar la TSF, entre los mandatos en el indicador `Thin server config>`.

Tabla 60. Resumen de mandatos de configuración de la TSF

Mandato	Función
? (Ayuda)	Visualiza todos los mandatos disponibles para este nivel de mandato, o lista las opciones de mandatos específicos (si es que están disponibles). Consulte "Obtención de ayuda" en la página xxv.
Add	Añade un servidor de archivos maestro (RFS o NFS).
Delete	Suprime un 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	Establece los parámetros del Thin Server.
Exit	Hace volver al nivel de mandato anterior. Consulte "Salida de un entorno de nivel inferior" en la página xxv.

Add

Utilice el mandato **add** para añadir la configuración de un servidor de archivos maestro.

Si selecciona *nfs* como tipo de servidor de archivos maestro, el Thin Server utilizará NFS para comunicar con el servidor de archivos maestro y sincronizar archivos y las NS se pueden comunicar con el Thin Server mediante TFTP o NFS. Si selecciona *rfs* como tipo de servidor maestro, el Thin Server utilizará RFS para comunicar con el servidor de archivos maestro y sincronizar archivos y las NS se pueden comunicar con el Thin Server mediante TFTP o RFS.

Sintaxis:

add master-file-server
nfs-s390
nfs-nt
nfs-aix
nfs-other
rfs-as400

nfs-s390
Se utiliza cuando la TSF se conecta a un S/390.

dirección IP del servidor de archivos

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 segmentos de paquetes.

Valores válidos: 512, 1024, 2048, 4096, 8192 (bytes)

Valor por omisión: 8192

additional Include subdirectories
Especifica si deben añadirse subdirectorios Include adicionales. Se pueden especificar subdirectorios adicionales si la TSF necesita guardar en antememoria archivos que no se encuentran en los directorios por omisión.

Valores válidos: yes (sí) o no

Valor por omisión: yes (sí)

additional Include subdirectory path
Especifica la vía de acceso del subdirectorio Include que se debe 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 de la vía de acceso del subdirectorio adicional especificado.

Valores válidos:

- No

  La TSF precargará todos los archivos del directorio especificado.
- Yes (Sí)

  La TSF no precargará ningún archivo del directorio especificado. La TSF cargará, en cambio, archivos del directorio y de cualquiera de sus subdirectorios, según convenga.

Valor por omisión: no

nfs-nt Se utiliza cuando la TSF se conecta 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 segmentos de paquetes.

Valores válidos: 512, 1024, 2048, 4096, 8192 (bytes)

Valor por omisión: 8192

additional Include subdirectories
Especifica si deben añadirse subdirectorios Include adicionales.

Valores válidos: yes (sí) o no

Valor por omisión: yes (sí)

additional Include subdirectory path
Especifica la vía de acceso del subdirectorio Include que se debe 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 de la vía de acceso del subdirectorio adicional especificado.

Valores válidos:

- No

  La TSF precargará todos los archivos del directorio especificado.
- Yes (Sí)

  La TSF no precargará ningún archivo del directorio especificado. La TSF cargará, en cambio, archivos del directorio y de cualquiera de sus subdirectorios, según convenga.

Valor por omisión: no

nfs-aix
Se utiliza cuando la TSF se conecta 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 segmentos de paquetes.

Valores válidos: 512, 1024, 2048, 4096, 8192 (bytes)

Valor por omisión: 8192

additional Include subdirectories
Especifica si deben añadirse subdirectorios Include adicionales.

Valores válidos: yes (sí) o no

Valor por omisión: yes (sí)

additional Include subdirectory path
Especifica la vía de acceso del subdirectorio Include que se debe 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 de la vía de acceso del subdirectorio adicional especificado.

Valores válidos:

- No

  La TSF precargará todos los archivos del directorio especificado.
- Yes (Sí)

  La TSF no precargará ningún archivo del directorio especificado. La TSF cargará, en cambio, archivos del directorio y de cualquiera de sus subdirectorios, según convenga.

Valor por omisión: no

nfs-other
Se utiliza cuando se desean 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 segmentos de paquetes.

Valores válidos: 512, 1024, 2048, 4096, 8192 (bytes)

Valor por omisión: 8192

additional Include subdirectories
Especifica si deben añadirse subdirectorios Include adicionales.

Valores válidos: yes (sí) o no

Valor por omisión: yes (sí)

additional Include subdirectory path
Especifica la vía de acceso del subdirectorio Include que se debe 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 de la vía de acceso del subdirectorio adicional especificado.

Valores válidos:

- No

  La TSF precargará todos los archivos del directorio especificado.
- Yes (Sí)

  La TSF no precargará ningún archivo del directorio especificado. La TSF cargará, en cambio, archivos del directorio y de cualquiera de sus subdirectorios, según convenga.

Valor por omisión: no

rfs-as400

Se utiliza cuando la TSF se conecta 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 segmentos de paquetes.

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 precarga.

Valores válidos: a-z, A-Z, 0-9, ., _, —, /

Valor por omisión:
/QIBM/ProdData/OS400/NetStationRmtController/LoadList.file

Ejemplo de 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 de 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 la configuración de un servidor de archivos maestro.

Sintaxis:

delete master-file-server
nfs
rfs

nfs Se utiliza cuando alguno de los servidores de archivos maestro NFS está configurado.

rfs Se utiliza cuando la TSF está configurada para el servidor de archivos maestro RFS.

List

Utilice el mandato **list** para visualizar la configuración de la 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 la configuración de un servidor de archivos maestro.

Sintaxis:

modify master-file-server
nfs

rfs

nfs Se utiliza cuando alguno de los servidores de archivos maestro NFS se ha configurado.

rfs Se utiliza cuando la TSF está configurada para el servidor de archivos maestro RFS.

Ejemplo de 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 de 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 establecer los parámetros de configuración de la TSF.

Sintaxis:

set mode
interval-pre-load-list
time-to-refresh-pre-load-list
memory-cache
hard-file

mode Especifica la modalidad de la TSF.

Valores válidos:

- enable

  Una modalidad "enable" significa que la TSF es totalmente funcional y que servirá archivos guardados en la antememoria a las Network Stations.

- disable

  Una modalidad "disable" significa que la TSF no está activa y que no responderá a ninguna Network Station. Las Network Stations deben estar configuradas para comunicar directamente con el servidor.
- passthru

  Una modalidad "passthru" sólo es válida si se utiliza RFS. Passthru permitirá que la Network Station contacte con la TSF, pero obtendrá siempre los archivos del servidor de archivos maestro.

Valor por omisión:

interval-pre-load-list
Especifica el intervalo de renovación de la lista de precarga en días.

Valores válidos: 00 - 365

Valor por omisión: 01

time-to-refresh-pre-load-list
Especifica la hora, en formato de 24 horas, a la que se debe renovar la antememoria.

Valores válidos: 0001 - 2400

Valor por omisión: 0100

memory-cache
Especifica la cantidad de memoria en megabytes de la antememoria RAM del Thin Server. Cuando se utiliza un disco fijo, se debe elegir este valor para equilibrar el rendimiento de la TSF con otras funciones del IBM 2212. Cuando no se utiliza un disco fijo, dicho valor debe ser lo suficientemente grande para contener todos los archivos guardados en memoria. Si desea obtener más información, consulte “Recomendaciones de configuración” en la página 551.

Valores válidos: 8 - 64 Megabytes

Valor por omisión: 16

hard-file
Especifica si se debe utilizar o no el disco fijo.

Valores válidos: yes (sí) o no

Valor por omisión: yes (sí)

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 la TSF

Utilice el procedimiento siguiente para acceder a los mandatos de supervisión de la TSF. Este proceso le proporciona acceso al proceso de *supervisión* de la TSF.

1. Entre **talk 5** en el indicador OPCON. (Si desea obtener más información sobre este mandato, consulte *The OPCON Process and Commands* en la publicación Software de Access Integration Services Guía del usuario.) Por ejemplo:

   ```
   * talk 5
   +
   ```

   Después de entrar el mandato **talk 5**, el indicador GWCON (+) aparece en el terminal. Si el indicador no aparece cuando entra por primera vez en la configuración, pulse **Intro** de nuevo.

2. Entre el mandato **f tsf** en el indicador + para acceder al indicador Thin-Server>.

   Ejemplo:

   ```
   + f tsf
   Thin-Server>
   ```

Mandatos de supervisión de la TSF

Esta sección describe los mandatos de supervisión de la TSF.

Tabla 61. Resumen de mandatos de supervisión de la TSF

Mandato	Función
? (Ayuda)	Visualiza todos los mandatos disponibles para este nivel de mandato, o lista las opciones de mandatos específicos (si es que están disponibles). Consulte “Obtención de ayuda” en la página xxv.
Delete	Suprime un archivo de la antememoria de archivos de la Thin Server Feature.
Flush	Vacía la antememoria de archivos de la Thin Server Feature.
List	Visualiza la configuración y los valores del Thin Server.
Refresh	Renueva la antememoria.
Reset	Restablece los contadores.
Restart	Reinicia el proceso del Thin Server.
Set	Cambia los valores de la Thin Server Feature.
Exit	Hace volver al nivel de mandato anterior. Consulte “Salida de un entorno de nivel inferior” en la página xxv.

Delete

Utilice el mandato **delete** para eliminar un archivo de la antememoria de archivos de la Thin Server Feature.

Sintaxis:

d**elete** *nombre_archivo*

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 vaciar la memoria de la TSF y el espacio de antememoria del disco duro. El mandato **flush** borrará todos los archivos guardados en la antememoria. La antememoria del Thin Server se actualizará en la próxima renovación a partir del servidor maestro. Las Network Stations pueden experimentar retrasos hasta que la renovación se complete.

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 los parámetros de la 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 identificadores tienen el siguiente significado:

- WhereFrom

  - — R = Cliente RFS
  - — N = Cliente NFS
  - — - = Ninguno
- InTable
  - — - = No en tabla
  - — u (o m) = A punto de actualizarse
  - — Y = En tabla
- FileState
  - — - = No en disco
  - — D = Sucio
  - — A = Actualización cancelada anormalmente
  - — u = A punto de actualizarse
  - — U = Actualización en proceso
  - — Y = En el disco y disponible

Las combinaciones habituales de los dos últimos identificadores (se muestran los tres identificadores para que resulte más claro) son:

- RYY - archivo bueno
- RuY - renovación completa en proceso, este archivo no se ha verificado todavía
- RYU - este archivo se está actualizando

Ejemplo de 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 de NFS

Mandatos de supervisión de la TSF (talk 5)

```
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 de RFS

```
Thin-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>
```

Ejemplo de 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 una renovación de la antememoria.

Sintaxis:

ref**resh**

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 restablecer dinámicamente contadores.

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 la TSF.

Sintaxis:

restart

Ejemplo:

```
Thin-Server> restart

Restart Thin Server? (Y/ [N]): y

Thin Server has been restarted
```

Set

Utilice el mandato **set** para establecer la modalidad de antememoria de la TSF.

Sintaxis:

set mode

mode Especifica la modalidad de la TSF. Consulte “Set” en la página 567.

Valores válidos:

- enable
- disable
- passthru

Ejemplo:

```
Thin-Server> set mode ?

DISABLED
ENABLED
PASSTHRU

Thin-Server> set mode disable

Thin Server caching is now disabled
```

Capítulo 34. Configuración y supervisión del VCRM

El gestor de recursos de circuito virtual (VCRM) es una función que ofrece soporte al protocolo de reserva de recursos (RSVP), el cual se describe en " Utilización de RSVP" y en "Configuración y supervisión de RSVP" en la publicación *Configuración y supervisión de protocolos - Manual de consulta Volumen 1*. A partir de la petición de reserva del RSVP, el VCRM crea la conexión del flujo de datos en la interfaz física. Para llevar a cabo esto, el VCRM debe determinar en primer lugar si existe suficiente ancho de banda para dar cabida a la reserva.

Nota: Si está utilizando interfaces WAN, como pueden ser Frame Relay o X.25, es necesario que establezca una velocidad de línea para que el VCRM sepa cuánto ancho de banda hay disponible. El procedimiento para establecer la velocidad de línea se describe en los capítulos de configuración y de supervisión de las interfaces Frame Relay y X.25 de la publicación *Software de Access Integration Services Guía del usuario.*

Si la interfaz es un enlace PPP, una LAN o una WAN, el VCRM utiliza la cola de software del QoS y los paquetes optimizados esfuerzo para asignar prioridades a los paquetes del enlace de salida.

Este capítulo consta de las siguientes secciones:

- "Acceso al entorno de configuración del VCRM"
- "Acceso al entorno de supervisión del VCRM"
- "Mandatos de supervisión del VCRM" en la página 576

Acceso al entorno de configuración del VCRM

Para acceder al entorno de configuración del 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 que se visualiza es indicar que el VCRM no se puede configurar de manera independiente. Al habilitar el RSVP, se habilita el VCRM, que obtiene sus parámetros de la configuración del RSVP.

Acceso al entorno de supervisión del VCRM

Para acceder al entorno de supervisión del 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 del VCRM

Esta sección describe los mandatos de supervisión del VCRM. Entre estos mandatos en el indicador `VCRM Console>`.

Tabla 62. Mandatos de supervisión del VCRM

Mandato	Función
? (Ayuda)	Visualiza todos los mandatos disponibles para este nivel de mandato, o lista las opciones de mandatos específicos (si es que están disponibles). Consulte “Obtención de ayuda” en la página xxv.
Clear	Restablece las estadísticas sobre colas.
Queue	Muestra estadísticas sobre colas de software.
Exit	Hace volver al nivel de mandato anterior. Consulte “Salida de un entorno de nivel inferior” en la página xxv.

Clear

Utilice el mandato **clear** para restablecer las estadísticas sobre colas de software.

Sintaxis:

clear

Consulte el mandato **queue** para ver un ejemplo del mandato **clear**.

Queue

Utilice el mandato **queue** para mostrar la cola de software de los flujos de tráfico .

Sintaxis:

queue

La lista siguiente define los términos que se utilizan en la visualización de las colas de software :

Quota
La cantidad de ancho de banda reservado. En un principio, B.E. (optimizado) dispone de todas las cuotas. Cuando se lleva a cabo una reserva, el ancho de banda (b/w) reservado se desplaza de la cuota B.E. a la cuota QoS.

Max-q
Longitud máxima de la cola, especificada en paquetes.

Curr-q
Longitud actual de la cola, especificada en paquetes.

In quota
Paquetes o kilobytes enviados dentro del ancho de banda asignado.

Outside quota
Paquetes o kilobytes enviados que superan el ancho de banda asignado, cuando no había ancho de banda desocupado disponible.

Packets/bytes dropped
Paquetes o bytes eliminados por la cola de software.

DLC packets/bytes dropped
Paquetes o bytes eliminados por DLC después de que los paquetes hayan pasado por 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/
        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>
```

Supervisión del VCRM (talk 5)

Capítulo 35. Utilización de los adaptadores de voz

Este capítulo describe el adaptador de voz y su utilización con el Nuera F200 Frame Relay Access Device (FRAD). La mayor parte del plan y configuración de marcación se efectúa en el F200. El F200 maneja todas las conexiones entre los puertos del 2212. La configuración de puertos del 2212 incluye sólo la información suficiente para acceder al F200.

Este capítulo consta de las siguientes secciones:

- "Visión general del adaptador de voz"
- "Configuración del Nuera F200 para la comunicación con un adaptador de voz del 2212" en la página 580
- "Configuración del puerto de voz 2212 para la comunicación con el Nuera F200" en la página 583
- "Comunicación sin utilizar un Nuera F200" en la página 584

Visión general del adaptador de voz

La Figura 50 en la página 580 muestra una red en la que dos 2212 están conectados con un Nuera F200 FRAD. Cada 2212 puede contener hasta cuatro tarjetas adaptadoras, cada una de las cuales contiene dos puertos de voz, lo que hace un total de ocho puertos. Los puertos pueden disponer de interfaces FXS, FXO, o E&M. Cada puerto de voz se puede conectar directamente a una central telefónica privada (PBX), a otro teléfono o a un sistema con teclado. Cada puerto de voz puede dar soporte a conexiones Frame Relay hasta un máximo de ocho F200. Los puertos de voz también se pueden conectar con otros puertos de voz dentro del mismo 2212. Ello se denomina *direccionamiento de llamadas locales.*

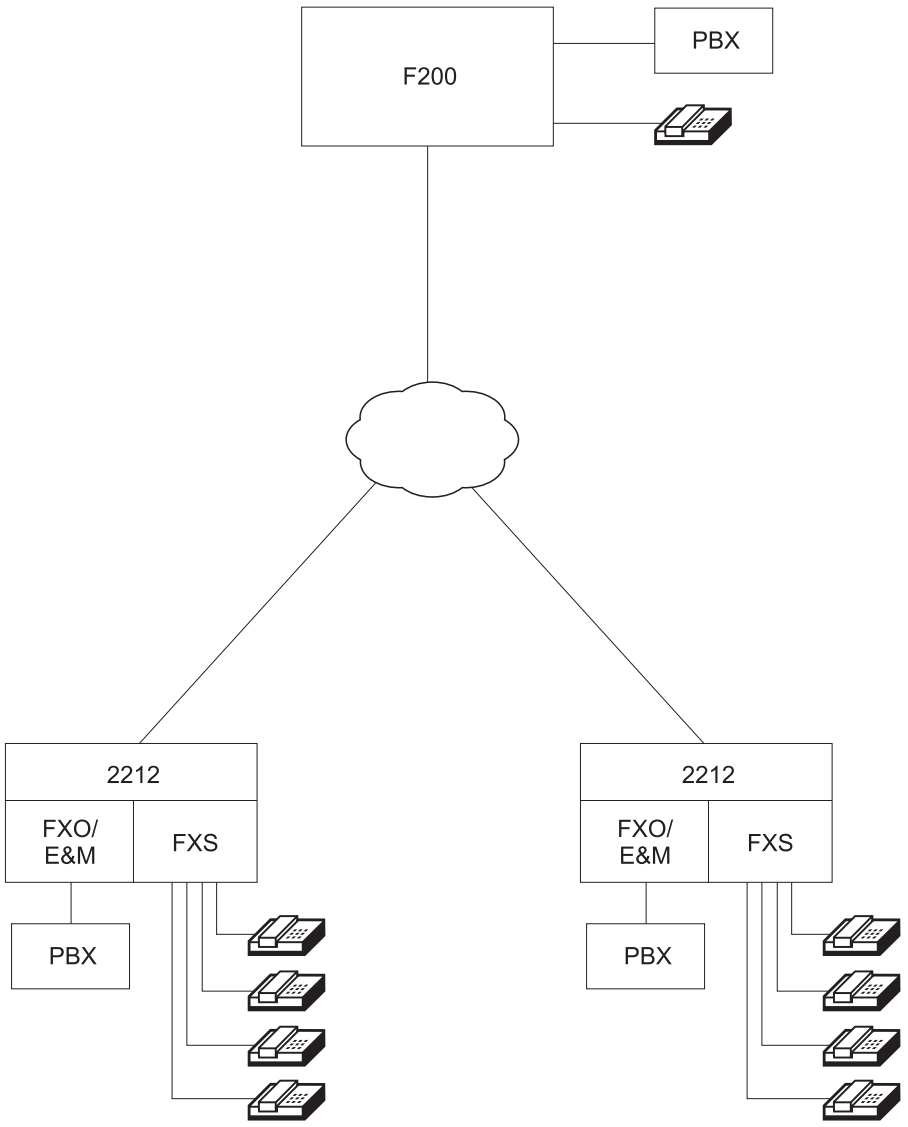


Figura 50. Comunicación entre los puertos de voz Nuera F200 y 2212

La definición del adaptador de voz es un proceso de configuración de dos pasos. En primer lugar, es necesario definir el F200 para que se comunique con el adaptador de voz 2212 y definir, a su vez, el puerto de voz 2212 para que se comunique con el F200.

Si desea ver ejemplos de definición de normas de proceso de llamadas, de coincidencias de marcación, de salida de red y de salidas telco, consulte el Capítulo 36, “Configuración y supervisión de los adaptadores de voz” en la página 587.

Configuración del Nuera F200 para la comunicación con un adaptador de voz del 2212

Para configurar el F200 para que se comunique con un adaptador de voz 2212, es necesario definir un conjunto de parámetros llamado *plan de marcación*. Un plan de marcación F200 contiene la siguiente información:

- Grupos de circuitos

- Descriptores de circuitos

La Figura 51 muestra la información de direccionamiento necesaria para la comunicación entre los puertos de voz de 2212A y 2212B.

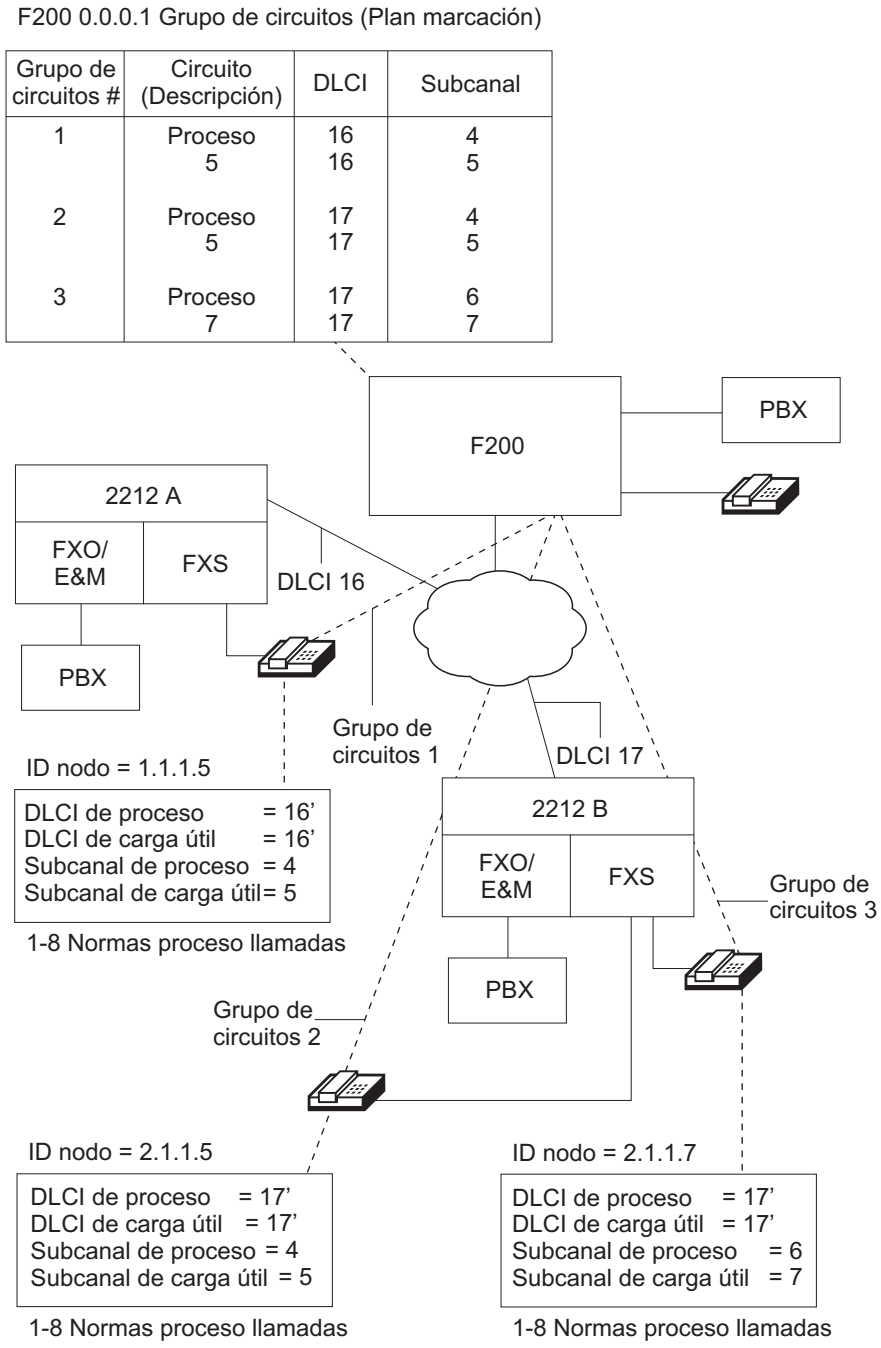


Figura 51. Configuración de la información del proceso de llamadas del puerto de voz

Un grupo de circuitos F200 define un *tronco de red de voz virtual* entre un F200 y un nodo remoto. Aunque un grupo de circuitos F200–F200 puede contener bastantes circuitos individuales, un grupo de circuitos de adaptadores de voz F200–2212 sólo contiene *un* circuito (PVC). El grupo de circuitos se conecta con el nodo remoto (el puerto de voz F200 o 2212). En la Figura 51, El Grupo de circuitos 1 se conecta con el puerto de voz 2212A que tiene el ID de nodo 1.1.1.5. El Grupo de circuitos 2 se conecta con el puerto de voz 2212B que tiene el ID de nodo 2.1.1.5. El Grupo de

circuitos 3 se conecta con el puerto de voz 2212B que tiene el ID de nodo 2.1.1.7. Cada puerto de voz 2212, incluso los puertos del mismo 2212, deben tener un ID de nodo exclusivo. Por lo tanto, se debe definir un grupo de circuitos exclusivo para cada puerto de voz 2212 del F200.

Un descriptor de circuitos F200 define los circuitos individuales dentro de cada grupo de circuitos. En el caso de un grupo de circuitos F200–F200, puede tener varios descriptores de circuitos; uno para cada circuito del grupo. Puesto que un grupo de circuitos de adaptadores de voz F200–2212 sólo contiene un circuito, un grupo de circuitos de adaptador de voz F200-2212 sólo contiene un descriptor de circuitos.

Los descriptores de circuitos contienen información tanto de *circuito de proceso* como de *circuito de carga útil*. El circuito de proceso se utiliza para transferir paquetes necesarios para establecer la llamada e interrumpirla. Dichos paquetes son los paquetes propietarios CALL SETUP, CONNECT, ANSWER y RELEASE de Nuera. El circuito de carga útil se utiliza para transferir paquetes que contienen los datos reales de voz comprimidos.

En la Figura 51 en la página 581, el F200 tiene un plan de marcación que contiene tres grupos de circuitos, uno para cada puerto de voz 2212. Cuando un F200 recibe una petición para establecer comunicación con un ID de nodo específico, utiliza el grupo de circuitos para localizar el dispositivo de destino. Un grupo de circuitos F200 contiene la siguiente información:

- El número del grupo de circuitos
- Nodo de conexión (nodo con el que se está conectando)
- Descriptores de circuitos (proceso y carga útil)
  - DLCI (16–991)
  - Subcanales (proceso y carga útil)

Nota: Cuando se define un descriptor de circuitos para un circuito de adaptador de voz F200–2212, el descriptor de circuitos y el número del subcanal de carga útil deben coincidir. El valor mínimo de subcanal que se puede especificar es 4. Todos los grupos de circuitos entre un F200 y un 2212 pueden utilizar el mismo DLCI.

Configuración de un plan de marcación

Un plan de marcación de un F200 consta de 1 a 4 normas de conversión. Dichas normas controlan el modo en que los dispositivos se conectan y se comunican con el F200. Cada norma de conversión consta de un número de *casos ordenados* (de 1 a 100). Cada grupo de circuitos F200 se asocia con una norma de conversión específica. Cada norma de conversión está compuesta de los siguientes elementos:

Norma de coincidencia de origen
Un patrón de coincidencia de dígitos de marcación para un número de origen

Norma de coincidencia de destino
Un patrón de coincidencia de dígitos de marcación para un número de destino

Norma de ruta
Una lista de grupos de circuitos, subconjuntos de grupos de circuitos o puertos locales.

Norma de salida de origen
Una norma para convertir el número de origen durante el establecimiento de la llamada.

Norma de salida de destino
Una norma para convertir el número de destino durante el establecimiento de la llamada o durante la transmisión de datos.

Durante el establecimiento de la llamada, los números de origen y destino se comparan con las normas de coincidencia correspondientes de cada caso de norma de conversión. Las comparaciones de efectúan en orden ascendente hasta que se encuentra una coincidencia. Cuando se encuentra una coincidencia, la norma de ruta del caso que ha coincidido direcciona la llamada. La norma de salida del caso que ha coincidido modifica la información del establecimiento de la llamada o genera dígitos de marcación.

Configuración del puerto de voz 2212 para la comunicación con el Nuera F200

Para configurar un puerto de voz 2212 para que se comunique con un F200, es necesario que defina las siguientes normas:

- Normas de salida telco — Una norma para cada puerto de voz
- Normas de proceso de llamadas — Hasta ocho normas para cada puerto de voz

Puede definir hasta ocho normas de salida telco para cada 2212 — una para cada puerto de voz. Las normas de salida telco determinan el modo en que los dígitos de marcación se transmiten en la interfaz telco. Cada norma telco consta de una combinación de dígitos de marcación de destino, dígitos de números de origen, constantes y pausas.

Puede definir hasta ocho normas de proceso de llamadas para cada puerto de voz. Cada norma contiene un conjunto de parámetros de conexión que determina el modo en que se establece una conexión. Cada norma de proceso de llamadas contiene la siguiente información:

- DLCI de proceso (16 a 1007)
- DLCI de carga útil (16 a 1007)
- Subcanal de proceso (4 a 254)
- Subcanal de carga útil (4 a 254)
- Número de norma de coincidencia de dígitos de marcación (1 a 64)
- Número de norma de salida de red (1 a 64)

Nota: Los parámetros de carga útil y de proceso definidos para un puerto de voz deben corresponder a los parámetros de carga útil y de proceso definidos para los F200 que se pueden conectar al puerto de voz.

La norma de coincidencia de dígitos de marcación le permite especificar el rango de dígitos aceptables en cada posición de una secuencia de dígitos de marcación. Puede especificar comodines de varios dígitos. así como una secuencia que establezca una conexión inmediata durante una condición de “descolgar”. Puede definir una agrupación de hasta 64 normas y especificar una norma de dígitos de marcación en cada norma de proceso de llamadas.

La norma de salida de red le permite especificar el modo en que el número de destino debe aparecer en el paquete Frame Relay de establecimiento de la llamada.

Dicha norma consta de una combinación de dígitos de número de destino y constantes.

Cuando un puerto de voz 2212 origina una llamada, el número de destino se compara con las normas de coincidencia de dígitos de marcación de ese puerto. Dichas normas se definen en las normas de proceso de llamadas de ese puerto. Cuando se encuentra una coincidencia, el DLCI y el subcanal de la norma de proceso de llamadas coincidente determinan el nodo de destino. Si el número de destino necesita ser modificado, la norma de salida de red determina el modo en que debe ser modificado.

Cuando un 2212 recibe una llamada, el par de DLCI y subcanal determina el puerto de voz que va a recibir la llamada. Cada puerto de voz acepta llamadas de cualquier par de DLCI y subcanal que esté definido en una de sus normas de proceso de llamadas. La norma de salida telco del puerto de voz de destino se utiliza con el número de destino para generar la secuencia de impulsos de marcación de salida, si ésta es necesaria.

Comunicación sin utilizar un Nuera F200

Si sólo necesita una accesibilidad limitada a la red, puede comunicar entre dos puertos de voz sin tener que utilizar un Nuera F200 gracias a los siguientes métodos:

- Comunicación entre los puertos de voz de diferentes 2212
- Comunicación entre los puertos de voz del mismo 2212 (direccionamiento de llamadas locales)

Comunicación de 2212 a 2212

Si se definen las correspondientes normas de proceso de llamadas para cada puerto de voz, se pueden efectuar llamadas entre dos puertos de voz de 2212 diferentes sin utilizar un F200. Cada una de dichas normas debe especificar los mismos subcanales de carga útil y de proceso de llamadas, así como los DLCI de carga útil y de proceso de llamadas correspondientes. Cuando se establece comunicación sin un F200, el campo de ID de nodo no se utiliza.

Nota: Sin conexión a un F200, cada puerto de voz se puede conectar a un máximo de ocho puertos de voz remotos. Si habilita el direccionamiento de llamadas locales en un puerto de voz, ese puerto de voz sólo se puede conectar a siete puertos de voz.

Direccionamiento de llamadas locales

Se pueden efectuar llamadas entre dos puertos de voz del mismo 2212 sin utilizar un F200. Ello se puede llevar a cabo configurando una de las ocho normas de proceso de cada puerto para el *direccionamiento de llamadas locales*. El direccionamiento de llamadas locales compara el número de destino con el número local configurado para cada puerto de voz que dispone de una norma de llamadas locales definida. Puede especificar el número de los dígitos iniciales que se deben comparar en el número local de cada puerto.

La norma de salida de red, especificada en una norma de llamada de ruta local, especifica los dígitos del número de destino necesarios para direccionar de manera correcta la llamada.

Puesto que los puertos de voz de origen y los puertos de voz de destino se encuentran dentro del mismo 2212, una norma de direccionamiento de llamadas locales no contiene información de DLCI ni de subcanal.

Utilización de un adaptador de voz

Capítulo 36. Configuración y supervisión de los adaptadores de voz

En este capítulo se describe cómo utilizar los mandatos de configuración y de funcionamiento del adaptador de voz, y consta de los apartados siguientes:

- "Acceso al entorno de configuración de la característica de voz"
- "Mandatos de configuración del adaptador de voz"
- "Mandatos de configuración de una red de voz" en la página 597
- "Acceso al entorno de supervisión del adaptador de voz" en la página 600
- "Mandatos de supervisión del adaptador de voz" en la página 600

Acceso al entorno de configuración de la característica de voz

Utilice el procedimiento siguiente para acceder al proceso de configuración del adaptador de voz.

1. En el indicador OPCON, escriba **talk 6** (si desea obtener más información sobre este mandato, consulte *The OPCON Process and Commands* en Software de Access Integration Services Guía del usuario). Por ejemplo:

   ```
   * talk 6
   Config>
   ```

   Después de escribir el mandato **talk 6**, aparecerá el indicador CONFIG (`Config>`) en la línea de mandatos. Si el indicador no aparece cuando se entra por primera vez la configuración, pulse **Intro** de nuevo.
2. En el indicador CONFIG, escriba el mandato **feat voice** para acceder al indicador `Voice Config>`.

Mandatos de configuración del adaptador de voz

En este apartado se describe cómo configurar el plan de marcación del 2212. También se describe cómo establecer los valores de los temporizadores y de los tonos, que se definen una sola vez para el 2212 pero son de aplicación para todos los puertos de voz del 2212.

Para configurar un adaptador de voz, escriba los mandatos siguientes en el indicador `Voice Config>`.

Tabla 63 (Página 1 de 2). Resumen de los mandatos de configuración de la característica de voz

Mandato	Función
? (Ayuda)	Visualiza todos los mandatos disponibles para este nivel de mandato, o lista las opciones de mandatos específicos (si es que están disponibles). Consulte "Obtención de ayuda" en la página xxv.
Add	Añade una norma de proceso de llamadas, de coincidencia de marcación, o de salida de red.
Delete	Elimina una norma de proceso de llamadas, de coincidencia de marcación, o de salida de red.
List	Lista los distintos valores de los temporizadores y de los tonos.

Tabla 63 (Página 2 de 2). Resumen de los mandatos de configuración de la característica de voz

Mandato	Función
Modify	Actualiza una norma de proceso de llamadas, de coincidencia de marcación, o de salida de red.
Reorder-Call-Rules	Cambia el orden de búsqueda de las normas de proceso de llamadas.
Set	Establece los temporizadores, los tonos y la Red-FR (red Frame Relay)
Exit	Hace volver al nivel de mandato anterior. Consulte “Salida de un entorno de nivel inferior” en la página xxv.

Add

Utilice el mandato **add** para añadir al adaptador de voz normas de proceso de llamadas, de coincidencia de dígitos de marcación y de salida de red.

Sintaxis:

add call-processing-rule
dial-matching-rule
network-output-rule
telco-output-rule

call-processing-rule

Especifica las normas de proceso de llamadas. Para las llamadas de salida, las normas de proceso de llamadas se evalúan en orden ascendente, comparando los dígitos marcados con la norma de coincidencia de dígitos de marcación asociada con cada norma de proceso de llamadas. Si se detecta una coincidencia, para procesar la llamada se utilizarán las normas de salida de red y de información de direccionamiento de llamada, de la norma de proceso de llamadas. Puesto que un puerto de voz puede aceptar llamadas de cualquiera de los destinos especificados en cualquiera de sus normas de información de direccionamiento de llamada asociadas, esta norma no tiene ningún efecto. Se pueden definir hasta ocho normas de proceso de llamadas para cada puerto de voz.

Nota: La norma de proceso de llamadas es equivalente a la norma de conversión del Nuera F200, que combina una norma de salida de red y una norma de coincidencia de marcación con la información de direccionamiento de llamada (especificación de DLCI y de subcanal, en caso de que la ruta de llamada sea remota, o dígitos del número de destino que se han de comparar con los números locales, en caso de que la ruta de llamada sea local).

```
Voice config>add call

Voice Net [0]? 5

Define Call Processing Rule #1

Destination Type (Local or Remote)(Remote?]?
Call Processing DLCI (16 to 1007)[16]?
Payload         DLCI (16 to 1007)[16]? 17
Call Processing Subchannel (4 to 254)[4]?
Payload         Subchannel (4 to 254)[4]? 5
Dial Digit Matching Rule (0 to 4)[1]?
Network Output Rule Number (0 to 2)[1]?
```

Destination Type

Especifica si el nodo de destino está en otro 2212/F200 (remoto) o en otro puerto de voz del mismo 2212 (local).

Call Processing DLCI
Especifica el DLCI que se utilizará para establecer e interrumpir la llamada.

Payload DLCI
Especifica el DLCI que se utilizará para enviar y recibir los paquetes de datos de voz comprimidos.

Call Processing Subchannel
Especifica el subcanal que se utilizará para establecer e interrumpir la llamada.

Payload Subchannel
Especifica el subcanal que se utilizará para enviar y recibir los paquetes de datos de voz comprimidos.

Dial Digit Matching Rule
Especifica el número de la norma de coincidencia de dígitos de marcación que utilizará esta norma de proceso de llamadas.

Network Output Rule
Especifica el número de la norma de salida de red que utilizará esta norma de proceso de llamadas.

dial-matching-rule
Especifica una secuencia de patrones de coincidencia de dígitos de marcación, en la que cada elemento de la secuencia especifica un rango de dígitos aceptables en esa posición.

Nota: La norma de coincidencia de marcación es equivalente a la norma de coincidencia de destino del Nuera F200.

```
Voice config>add dial

Define Dial Digit Matching Rule #4

Dial Mask 1: Digit String (0-9, A-D, *, #), [W]ildcard, [N]umeric Wildcard,
                                             [M]ultidigit Wildcard
             [MultiDigit Wildcard]? 456    /* se compara con el 4, el 5 y el 6 */
Dial Mask 2: Digit String (0-9, A-D, *, #), [W]ildcard, [N]umeric Wildcard,
                                             [M]ultidigit Wildcard, or [E]nd
             [End]? m
Dial Mask 3: Digit String (0-9, A-D, *, #), [W]ildcard, [N]umeric Wildcard,
                                             [M]ultidigit Wildcard
             [MultiDigit Wildcard]? e

Matching Rule contains Multidigit Wildcard(s)
Minimum number  of digits accepted for Multidigit Wildcard [1]?    (specify either 0 or 1)
```

Dial Mask núm.
Especifica una de las veinte máscaras de dígitos de marcación posibles. Cada máscara indica el rango aceptable del dígito en esta posición de la secuencia de marcación de 20 dígitos.

Digit String
Especifica un conjunto de dígitos del que debe elegirse el dígito.

Wildcard
Especifica que el dígito debe ser uno de los siguientes: 0–9, A—D, # o *.

Numeric Wildcard
Especifica que el dígito debe estar comprendido entre el 0 y el 9

Multidigit Wildcard
Especifica que en la posición especificada se puede aceptar más de un dígito. Si la máscara de comodín de varios dígitos es la última de la norma de coincidencia de marcación, se podrá entrar cualquier dígito (0–9, A—D, #, *) en este punto de la secuencia. En este caso, el puerto de voz continuará captando dígitos hasta que se entren los 20 dígitos o hasta que se agote el tiempo de espera entre dígitos sin que se haya entrado ningún otro dígito. Si hay una máscara después del comodín de varios dígitos, el puerto de voz continuará captando dígitos que satisfagan la máscara de varios dígitos hasta que se entre un dígito que satisfaga la máscara que hay después del comodín de varios dígitos.

network-output-rule
Especifica los dígitos del número de destino que se pasarán en el paquete de establecimiento de llamada Frame Relay. La secuencia se especifica como una combinación de constantes y de los dígitos marcados recibidos en el puerto telco de origen.

Nota: La norma de salida de red es equivalente a la norma de salida de destino del Nuera F200 para un puerto Frame Relay.

```
Voice config>add network

Define Network Output Rule #5

Digit 1: (Destination/Constant/End) [End]? c
         (0-9, A-D, *, #) [0]? 1
Digit 2: (Destination/Constant/End) [End]?
         (1-20) [1]?
Digit 3: (Destination/Constant/End) [End]?
         (1-20) [2]?
Digit 4: (Destination/Constant/End) [End]?
         (1-20) [3]?
Digit 5: (Destination/Constant/End) [End]? e
```

Digit núm.
Especifica cómo se determina el dígito de marcación concreto.

Destination
Se ha de utilizar el dígito de la posición especificada del número de teléfono de destino.

Constant
Se ha de utilizar siempre el dígito constante siguiente (0–9, A—D, #, *) en la posición especificada.

End Especifica el final de la secuencia de dígitos.

telco-output-rule
Especifica la secuencia de dígitos de marcación que se enviarán desde el puerto telco cuando éste sea el destino de una llamada. La secuencia se especifica como una combinación de constantes, de caracteres de pausa y de los dígitos de marcación de los números de origen y de destino enviados durante el establecimiento de llamada.

Nota: La norma de salida es equivalente a la norma de salida de destino del Nuera F200 para un puerto de voz.

```
Voice config>add telco

Define Telco Output Rule #4

Digit 1: (Source/Destination/Constant/Pause/End) [Destination]? c
         (0-9, A-D, *, #) [0]? 9
Digit 2: (Source/Destination/Constant/Pause/End) [Destination]? p
Digit 3: (Source/Destination/Constant/Pause/End) [Destination]?
         (1-40) [1]?
Digit 4: (Source/Destination/Constant/Pause/End) [Destination]?
         (1-40) [2]?
Digit 5: (Source/Destination/Constant/Pause/End) [Destination]?
         (1-40) [3]?
Digit 6: (Source/Destination/Constant/Pause/End) [Destination]? e
```

Digit núm.
Especifica cómo se determina el dígito de marcación concreto.

Source
Se ha de utilizar el dígito de la posición especificada del número de teléfono de origen.

Destination
Se ha de utilizar el dígito de la posición especificada del número de teléfono de destino.

Source
Se ha de utilizar el dígito de la posición especificada del número de teléfono de origen.

Constant
Se ha de utilizar siempre el dígito constante siguiente (0–9, A—D, #, *) en la posición dada.

Pause En este punto de la secuencia de dígitos de marcación, se ha de insertar un intervalo de pausa.

End Especifica el final de la secuencia de dígitos.

Delete

Utilice el mandato **delete** para suprimir del adaptador de voz, normas de proceso de llamadas, de coincidencia de dígitos de marcación y de salida de red.

Sintaxis:

delete
- call-processing-rule
- dial-matching-rule
- network-output-rule
- telco-output-rule

Para obtener una explicación de las normas de proceso de llamadas, de coincidencia de marcación y de salida de red, consulte “Add” en la página 588.

List

Utilice el mandato **list** para visualizar información sobre las normas, los retardos de los temporizadores y los valores de los tonos.

Sintaxis:

list
- call-processing-rule
- dial-matching-rule
- network-output-rule
- telco-output-rule
- timers

tones

call processing rule
Lista la norma de proceso de llamadas del puerto de voz especificado. Si no se especifica el número de puerto, aparecerá el indicador `Voice Net [0]`, donde podrá especificarlo.

```
Voice config>list call

Voice Net [0]? 5

Call Processing Rule #1

Call Processing DLCI       =16
Payload         DLCI       =17
Call Processing Subchannel = 4
Payload         Subchannel = 5
Dial Digit Matching Rule   = 1
Network Output      Rule   = 1
```

Call processing DLCI
Indica el DLCI de proceso de llamadas definido para este puerto.

Payload DLCI
Indica el DLCI de carga útil definido para este puerto.

Call processing subchannel
Indica el subcanal de proceso de llamadas definido para este puerto.

Payload subchannel
Indica el subcanal de carga útil definido para este puerto.

Dial digit matching rule
Indica la norma de coincidencia de dígitos de marcación que está utilizando actualmente este puerto.

Network output rule
Indica la norma de salida de red que está utilizando actualmente este puerto.

dial matching rule
Lista la norma de coincidencia de dígitos de marcación del puerto de voz especificado. Si no se especifica el número de puerto, aparecerá el indicador `Voice Net [0]`, donde podrá especificarlo.

```
Voice config>list dial 4

Dial Digit Matching Rule #4

Dial Mask 1:Match Digits=456
Dial Mask 2:Match Digits=MultiDigit Wildcard
```

network-output-rule
Lista la norma de proceso de red del puerto de voz especificado.

telco-output-rule
Lista la norma de salida telco del puerto de voz especificado.

timers Lista todos los retardos y tiempos de espera (en milisegundos) asociados con este adaptador de voz. Estos parámetros se describen en la página 594.

```
Voice config>list timers

Seize Detect Delay    :50   ms   First Digit Timeout     :10000 ms
Answer Detect Delay   :10   ms   Inter Digit Timeout     :5000  ms
Discon Detect Delay   :200  ms   Start Dial Delay        :500   ms
Glare Detect Delay    :500  ms   Ring No Answer Timeout  :30000 ms
Wink Detect Timeout   :2000 ms   Ring on Detect Timeout  :400   ms
Wink Start Delay      :50   ms   Ring Off Detect Timeout :6000  ms
Wink Duration         :200  ms   Warble Timeout          :10000 ms
```

tones Lista todos los tonos asociados con este adaptador de voz. Estos parámetros se describen en la página 595.

```
Voice config>list tones

Tone         On1    Off1    On2   Off2   Freq1 Freq2   Level1 Level2
             ms     ms      ms    ms     Hz    Hz      dB     dB
Dial         0      0       0     0      350   440     -16    -16
Ring Back    2000   4000    2000  4000   440   480     -22    -22
Busy         500    500     500   500    480   620     -20    -20
Fast Busy    300    300     300   300    480   620     -16    -16
Warble       100    100     100   100    1400  2060    -16    -16
Dtmf         100    100                                -7
```

Modify

Utilice el mandato **modify** para actualizar las normas de proceso de llamadas, de coincidencia de dígitos de marcación y de salida de red, del adaptador de voz.

Sintaxis:

modify call-processing-rule
dial-matching-rule
network-output-rule
telco-output-rule

Para obtener una explicación de las normas de proceso de llamadas, de coincidencia de marcación y de salida de red, consulte “Add” en la página 588.

Reorder-Call-Rule

Utilice el mandato **reorder-call-rule** para cambiar el orden de búsqueda de las normas de proceso de llamadas.

Sintaxis:

reorder-**call-rule** número_red núm_norma_antigua núm_norma_nueva

número_red
Especifica el número de la red de la que se quiere cambiar el orden de las normas de proceso de llamadas.

núm_norma_antigua
Especifica el número actual (1–8) de la norma de proceso de llamadas que se quiere cambiar de orden.

núm_norma_nueva
Especifica en qué lugar (1–8) de la nueva lista de normas de proceso de llamadas debe aparecer la norma que se quiere cambiar de orden.

En el ejemplo siguiente, la sexta norma de la lista de normas de proceso de llamadas de la red 5, pasará a ser la primera norma de la lista.

```
Voice config>reorder call-rule 5 6 1
```

Set

Utilice el mandato **set** para especificar los valores de los retardos y tiempos de espera.

Sintaxis:

set fr-net *número_red*
timer ...

tone ...

fr-net Utilice el mandato **fr-net** para especificar el número de red Frame Relay a través de la que se direccionarán los paquetes VoFR (trama de voz). Especifique cualquier número de red configurada o 0X'FFFF', si no se especifica ninguna red.

timer Utilice el mandato **set timer** para establecer los siguientes parámetros de un temporizador.

answer-detect-delay
Tiempo (en milisegundos) que transcurrirá antes de que se reconozca una señal de respuesta. Los valores posibles están comprendidos entre 0 y 500 milisegundos. El valor por omisión es de 10 milisegundos.

disconnect-detect-delay
Tiempo (en milisegundos) que transcurrirá antes de que se reconozca una señal de desconexión. Los valores posibles están comprendidos entre 0 y 500 milisegundos. El valor por omisión es de 200 milisegundos.

first-digit-timeout
Tiempo (en milisegundos) durante el que debe recibirse el primer dígito. Los valores posibles están comprendidos entre 0 y 10.000 milisegundos. El valor por omisión es de 10.000 milisegundos.

glare-detect-delay
Tiempo (en milisegundos) que transcurrirá antes de que un puerto pueda tomar un canal. Los valores posibles están comprendidos entre 0 y 500 milisegundos. El valor por omisión es de 500 milisegundos.

inter-digit-timeout
Tiempo (en milisegundos) durante el que debe recibirse un dígito *después* de haber recibido el primero. Los valores posibles están comprendidos entre 0 y 10.000 milisegundos. El valor por omisión es de 500 milisegundos.

ring-no-answer-timeout
Tiempo (en milisegundos) que esperará respuesta un canal de voz que llame a un puerto FXO, antes de renunciar a la llamada. Los valores posibles están comprendidos entre 0 y 64.000 milisegundos. El valor por omisión es de 30.000 milisegundos.

ring-off-detect-timeout
Tiempo (en milisegundos) durante el que no debe haber señal de llamada en un puerto FXO, para que el servidor determine que la llamada se ha interrumpido. Los valores posibles están comprendidos entre 0 y 64.000 milisegundos. El valor por omisión es de 6.000 milisegundos.

ring-on-detect-timeout
Tiempo (en milisegundos) durante el que ha de haber señal de llamada en un puerto FXO, para que se reconozca la llamada. Los valores posibles están comprendidos entre 0 y 64.000 milisegundos. El valor por omisión es de 400 milisegundos.

seize-detect-delay
Tiempo (en milisegundos) que transcurrirá antes de que se reconozca una señal de toma. Los valores posibles están comprendidos entre 0 y 500 milisegundos. El valor por omisión es de 50 milisegundos.

start-dial-delay
Tiempo (en milisegundos) que transcurrirá después de recibir una señal de marcación, pero antes de transmitir los dígitos. Los valores posibles están comprendidos entre 0 y 64.000 milisegundos. El valor por omisión es de 500 milisegundos.

warble-timeout
Tiempo (en milisegundos) de silencio que debe transcurrir después de una desconexión, para poder generar una señal de frecuencia variable. Los valores posibles están comprendidos entre 0 y 64.000 milisegundos. El valor por omisión es de 10.000 milisegundos.

wink-detect-timeout
Tiempo (en milisegundos) que debe transcurrir sin recibir una señal de guiño, antes de que se interrumpa la llamada. Los valores posibles están comprendidos entre 0 y 64.000 milisegundos. El valor por omisión es de 2.000 milisegundos.

wink-duration
Duración (en milisegundos) de la señal de guiño. Los valores posibles están comprendidos entre 0 y 10.000 milisegundos. El valor por omisión es de 200 milisegundos.

wink-start-delay
Tiempo (en milisegundos) transcurrido después de recibir una señal entrante de toma antes de generar una señal de guiño. Los valores posibles están comprendidos entre 0 y 64.000 milisegundos. El valor por omisión es de 50 milisegundos.

tone Utilice el mandato **set tone** para establecer los parámetros de tono siguientes.

busy Especifica las características de hasta dos frecuencias, utilizadas para generar la señal de ocupado. Al entrar el mandato set tone busy, se le pedirá la información siguiente:

on1 Tiempo (en milisegundos) que la frecuencia *freq1* estará "activa". Si el valor especificado es cero, el tono asociado estará siempre activado, lo que produce un tono continuo. Los valores posibles están comprendidos entre 0 y 32.767 milisegundos. El valor por omisión es cero.

off1 Tiempo (en milisegundos) que la frecuencia *freq1* estará "inactiva". Si el valor especificado es cero, el tono asociado estará siempre activado, lo que produce un tono continuo. Los valores posibles están comprendidos entre 0 y 32.767 milisegundos. El valor por omisión es cero.

on2 Tiempo (en milisegundos) que la frecuencia *freq2* estará "activa". Si el valor que se especifica es cero, el tono asociado estará siempre activado, lo que equivale a un tono continuo. Los valores posibles están comprendidos entre 0 y 32.767 milisegundos. El valor por omisión es cero.

off2 Tiempo (en milisegundos) que la frecuencia *freq2* estará "inactiva". Si el valor que se especifica es cero, el tono asociado estará siempre activado, lo que equivale a un tono continuo. Los valores posibles están comprendidos entre 0 y 32.767 milisegundos. El valor por omisión es cero.

freq1 Frecuencia (en hercios) del primer tono de la señal de ocupado. Los valores posibles están comprendidos entre 0 y 3.000 hercios. El valor por omisión es de 350 hercios.

freq2 Frecuencia (en hercios) del segundo tono de la señal de ocupado. Los valores posibles están comprendidos entre 0 y 3.000 hercios. El valor por omisión es de 440 hercios.

level1 Nivel de ganancia, en decibelios, de la frecuencia *freq1*, en incrementos de 0,5 dB. Los valores posibles están comprendidos entre los –13dB y los –40 dB. El valor por omisión es de –16 dB.

level2 Nivel de ganancia, en decibelios, de la frecuencia *freq2*, en incrementos de 0,5 dB. Los valores posibles están comprendidos entre los –13dB y los –40 dB. El valor por omisión es de –16 dB.

dial Especifica las características de hasta dos frecuencias utilizadas para generar un tono de marcación. Cuando se entra el mandato **set tone dial**, se le pedirán los datos siguientes: *on1*, *off1*, *on2*, *off2*, *freq1, freq2, level1 y level2*. Estos parámetros se describen en la página 595.

dtmf Especifica las características de la señal de multifrecuencia de dos tonos (DTMF). Cuando se entra el mandato **set tone dtmf**, se le pedirá la información siguiente:

ontime
Especifica el "tiempo que estará activada" (en milisegundos) la señal DTMF. Si el valor que se especifica es cero, no se generará ninguna señal DTMF. Normalmente no debe especificarse un *tiempo que estará activada* de menos de 40 milisegundos. Esto genera una señal de 12,5 tonos por segundo. Los valores posibles están comprendidos entre 0 y 32.767 milisegundos. El valor por omisión es de 100 milisegundos.

offtime
Especifica el "tiempo que estará desactivada" (en milisegundos) la señal DTMF. Si el valor que se especifica es cero, no se generará ninguna señal DTMF. Los valores posibles están comprendidos entre 0 y 32.767 milisegundos. El valor por omisión es de 100 milisegundos.

level Especifica el nivel de ganancia, en decibelios, de la señal DTMF en incrementos de 0,5 dB. Los valores posibles están comprendidos entre los –7 dB y los –25 dB. El valor por omisión es de –7 dB.

fast busy
Especifica las características de hasta dos frecuencias utilizadas para generar la señal rápida de ocupado. Cuando se entra el mandato **set tone fast busy**, se le pedirán los datos siguientes *on1, off1, on2, off2, freq1, freq2, level1 y level2*. Estos parámetros se describen en la página 595.

ring-back
Especifica las características de hasta dos frecuencias utilizadas para generar un eco. Cuando se entra el mandato **set tone ring-back**, se le pedirán los datos siguientes: *on1, off1, on2, off2, freq1, freq2, level1 y level2*. Estos parámetros se describen en la página 595.

warble
Especifica las características de hasta dos frecuencias utilizadas para generar un tono de marcación. Cuando se entra el mandato **set tone warble**, se le pedirán los datos siguientes: *on1, off1, on2, off2, freq1, freq2, level1 y level2*. Estos parámetros se describen en la página 595.

Mandatos de configuración de una red de voz

Para configurar una red de voz, escriba el mandato **network** junto con el número de puerto de voz.

```
Config> network 5
Voice 5 Config>
```

Para configurar un adaptador de voz, escriba los mandatos siguientes en el indicador `Voice n Config>`.

Tabla 64. Resumen de mandatos del puerto de voz

Mandato	Función
? (Ayuda)	Visualiza todos los mandatos disponibles para este nivel de mandato, o lista las opciones de mandatos específicos (si es que están disponibles). Consulte “Obtención de ayuda” en la página xxv.
List	Lista varios valores del puerto de voz.
Set	Establece varios parámetros del puerto de voz.
Exit	Hace volver al nivel de mandato anterior. Consulte “Salida de un entorno de nivel inferior” en la página xxv.

List

Utilice el mandato **list** para visualizar los valores actuales de un puerto de voz.

Sintaxis:

list

Por ejemplo, para listar la configuración actual del puerto de voz, escriba:

```
Voice 5 config>list

NodeID: 1.2.3.4

Local Phone Number:1234567

Telco Output Rule Number: 0

Telco Parameters

Tx Gain   :-4 dB       E&M Type :1
Rx Gain   :-4 dB       E&M Wire :4
OOS Signal:Busy        E&M Start:Immediate

Dsp Parameters

Vocoder Suite :Nuera   VAD Mode      :Off
Vocoder Rate  :9600    VAD Hangover  :255 ms
Frame Packing :1       VAD Threshold :-45 dB

Echo Cancel   :On      Fax   :On
NLP           :On      NSF   :On
2100Hz Detect :On
```

Node ID
Indica el ID de nodo del Nuera del puerto de voz.

Local Telephone Number
Indica el número de teléfono local del puerto de voz.

Telco Output Rule
Indica la norma de salida telco que está utilizando actualmente el puerto de voz.

Tx Gain
Indica la ganancia actual de transmisión, en decibelios.

Rx Gain
Indica la ganancia actual de recepción, en decibelios.

OOS Signal
Indica el tipo de señal que se utilizará si el puerto no funciona.

E&M Type
Indica el tipo de interfaz telco que utiliza el puerto de voz.

E&M Wire
Indica si el puerto de voz es de 2 o de 4 hilos.

E&M Start
Indica cómo iniciará la transmisión el puerto de voz.

Vocoder Suite
Indica la suite del vocoder (ITU o NUERA) disponible actualmente para el puerto de voz.

Vocoder Rate
Indica la cadencia actual del vocoder.

VAD Mode
Indica el tipo de VAD que se está utilizando. Se puede especificar fijo, adaptativo o ninguno.

VAD Hangover
Indica el tiempo que el nivel de la señal de entrada debe permanecer por debajo del valor umbral VAD antes de considerar que el enlace está mudo.

VAD Threshold
Indica el nivel de la señal (en decibelios) que se utilizará para determinar cuándo está mudo un enlace.

NLP Indica si el proceso no lineal está habilitado (On) o inhabilitado (Off).

2100Hz Detect
Indica si la detección de los 2100Hz está habilitada (On) o inhabilitada (Off).

FAX Indica si la característica FAX Relay está habilitada (On) o inhabilitada (Off).

NSF Indica si los recursos no estándar están habilitados (On) o inhabilitados (Off).

Consulte la página 598 para obtener la descripción de más parámetros adicionales.

Set

Utilice el mandato **set** para especificar los valores de un determinado puerto de voz.

Sintaxis:

set echo-cancel
frame-packing
local-number
node-id
oos

output-rule
rate
rx-gain
start
suite
tx-gain
vad
wire

Se pueden especificar los parámetros siguientes para el mandato **set**:

echo-cancel
Especifica si se habilita o no la cancelación de eco. Se puede elegir entre *yes (sí)* (1) y *no* (2). El valor por omisión es *yes*.

frame-packing
Especifica el número de tramas de voz que se empaquetarán en un único paquete Frame Relay. Los valores posibles están comprendidos entre 1 y 5. El valor por omisión es 1.

local-number
Especifica el número de teléfono local del puerto de voz especificado. Los valores posibles son cualquier número de 20 dígitos (de 0 a 9, de A a D, *, #). El valor por omisión es 0.

node-id
Especifica el ID de nodo del Nuera del puerto. El valor por omisión es 0.0.0.0.

oos Especifica el tipo de tono que se quiere utilizar para indicar que el puerto de voz especificado no funciona. Se puede elegir entre *idle (desocupado)* (1) o *busy (ocupado)* (2). El valor por omisión es *busy*.

output-rule
Especifica qué norma de salida telco se utilizará. Los valores posibles están comprendidos entre 0 y 8 (el límite superior depende del número de normas de salida Telco que se hayan definido). El valor por omisión es 0.

rate Especifica la velocidad de transmisión del puerto de voz. Si se especifica Nuera como parámetro de la suite, se pueden elegir los valores siguientes: 4,8 KB; 7,47 KB; 9,6 KB o 32 KB. Si se especifica ITU como parámetro de la suite, se pueden elegir los valores siguientes: 8 KB, 16 KB o 32 KB. El valor por omisión es 9,6 KB.

rx-gain
Especifica el valor en que el puerto de voz atenúa (o amplifica) la señal recibida. Los valores posibles están comprendidos entre –16 dB y +7 dB. El valor por omisión es de –4 dB.

start (E&M-only)
Especifica cómo iniciará las transmisiones el puerto de voz. Se puede elegir entre *immediate start (inicio inmediato)* (1) o *wink start (inicio de guiño)* (2). El valor por omisión es *immediate start*.

suite Especifica el tipo de protocolo que quiere que utilice el puerto de voz. Se puede elegir entre *NUERA — ECELP/G.726* (2) o *ITU — G.729/G728/G.726* (3). El valor por omisión es *NUERA*.

tx-gain
Especifica el valor en que el puerto de voz atenúa (o amplifica) la señal transmitida. Los valores posibles están comprendidos entre –16 dB y +7 dB. El valor por omisión es de —4 dB.

Mandatos de supervisión del adaptador de voz (talk 5)

type (E&M-only)
Especifica la interfaz E&M telco para el puerto de voz especificado. Se puede elegir entre 1, 2 ó 5. El valor por omisión es 1.

vad Especifica la modalidad VAD. Se puede elegir entre *fixed (fija)* (1), *adaptive (adaptativa)* (2), o *none (ninguna)* (3). El valor por omisión es *adaptive*.

wire (E&M-only)
Especifica si la conexión telco que se está utilizando es de 2 o de 4 hilos. El valor que se puede especificar es 2 (2 hilos) o 4 (4 hilos). El valor por omisión es 4.

Acceso al entorno de supervisión del adaptador de voz

Utilice el procedimiento siguiente para acceder a los mandatos de supervisión del adaptador de voz. Este proceso le proporciona acceso al proceso de *supervisión* del adaptador de voz.

1. Entre **talk 5** en el indicador OPCON (si desea obtener más información sobre este mandato, consulte *The OPCON Process and Commands* en Software de Access Integration Services Guía del usuario). Por ejemplo:

   ```
   * talk 5
   +
   ```

   Después de entrar el mandato **talk 5**, aparecerá el indicador GWCON (+) en la línea de mandatos. Si el indicador no aparece cuando se entra por primera vez la configuración, pulse **Intro** de nuevo.

2. Entre el mandato **network n** en el indicador + para acceder al indicador `Voice n Console >`.

   Ejemplo:

   ```
   + network 2
   Voice 2 Console>
   ```

Mandatos de supervisión del adaptador de voz

En este apartado se describen los mandatos de supervisión del adaptador de voz.

Tabla 65. Resumen de mandatos de supervisión del adaptador de voz

Mandato	Función
? (Ayuda)	Visualiza todos los mandatos disponibles para este nivel de mandato, o lista las opciones de mandatos específicos (si es que están disponibles). Consulte “Obtención de ayuda” en la página xxv.
Calls	Muestra varios contadores de sucesos y mensajes asociados con el puerto de voz especificado.
Status	Muestra varios valores del puerto de voz, así como información sobre los errores de transmisión o recepción.
Trace call	Muestra información de rastreo sobre una interfaz de destino.
Exit	Hace volver al nivel de mandato anterior. Consulte “Salida de un entorno de nivel inferior” en la página xxv.

Calls

Utilice el mandato **calls** para visualizar los mensajes de proceso de llamadas y los contadores de sucesos.

Sintaxis:

calls

Ejemplo:

```
Voice 1 Console> calls

Event Counters

Seize Detected              5           Digit Detected       4
Seize Applied               0           Digit Generated     0

Message Counters

Setup Sent                  1           Setup Received       0
Connect Sent                0           Connect Received     1
Answer Sent                 0           Answer Received      1
Release Sent                2           Release Received     0

Release Cause Counters

Normal                      1            Response            0
Busy                        1            OOS                 0
Local Bandwidth             0            Incompatible        0
Remote Bandwidth            0
```

Event Counters

Indican el número de sucesos producidos en la interfaz telco.

Seize Detected

Indica el número de sucesos Seize In (el teléfono conectado al puerto de voz se desconecta—cuelga).

Seize Applied

Indica el número de sucesos Seize Out (el propio puerto de voz se desconecta—cuelga).

Digit Detected

Indica el número de dígitos de marcación recibidos del abonado en la interfaz telco.

Digit Generated

Indica el número de dígitos de marcación enviados al abonado en la interfaz telco.

Message Counters

Indican el número de mensajes de proceso de llamadas enviados a un puerto de voz o recibidos por éste, a través del circuito Frame Relay. Cuando se establece una llamada, se envían mensajes de Establecimiento, Conexión y Respuesta entre los dos nodos. El iniciador de la llamada envía un mensaje de Establecimiento al extremo remoto, que responde con un mensaje de Conexión seguido de un mensaje de Respuesta, si la llamada es satisfactoria. Si la llamada no puede realizarse, el nodo remoto enviará un mensaje de Liberación. Cada extremo también envía mensajes de Liberación cuando una llamada satisfactoria finaliza normalmente (ambos nodos se conectan y cuelgan).

Setup Sent

Indica el número de mensajes de Establecimiento enviados.

Connect Sent
Indica el número de mensajes de Conexión enviados.

Answer Sent
Indica el número de mensajes de Respuesta enviados.

Release Sent
Indica el número de mensajes de Liberación enviados.

Setup Received
Indica el número de mensajes de Establecimiento recibidos.

Connect Received
Indica el número de mensajes de Conexión recibidos.

Answer Received
Indica el número de mensajes de Respuesta recibidos.

Release Received
Indica el número de mensajes de Liberación recibidos.

Release Cause Counters
Indican las causas del mensaje de Liberación.

Normal
Indica el número de señales de colgar normales iniciadas por el nodo local.

Busy Indica el número de señales de colgar causadas por un canal ocupado.

Local Bandwidth
Indica el número de señales de colgar causadas por un ancho de banda local insuficiente.

Remote Bandwidth
Indica el número de señales de colgar causadas por un ancho de banda remota insuficiente.

Response
Indica el número de señales de colgar normales iniciadas por el nodo remoto.

OOS Indica el número de señales de colgar causadas porque el nodo remoto no funciona.

Incompatible
Indica el número de señales de colgar causadas por incompatibilidad con el nodo remoto.

Status

Utilice el mandato **status** para visualizar información sobre un puerto de voz especifico.

Sintaxis:

status

Ejemplo:

```
Voice 1 Config> status

Node ID             :0.0.0.0
Absolute Port Address    :01

Vocoder Suite         Nuera           Echo Canceller      Filter
Vocoder Active        ECELP           Fax Demodulation    Idle
Vocoder Rate           9600           Fax Modulation      Idle
Vocoder Packet Size      18           Fax Type            V.27 at 9600 bps
Vocoder Frame Size      120           Fax Last FCF        0

Last Received    Dial Sequence       :8675309
Last Transmitted Dial Sequence       :911

Transmit Packets                Receive Packets

Total           179             Total       184
Voice           169             Voice       167
CAS               0             CAS          11
DTMF              0             DTMF          0
FAX               0             FAX           0
Lost              0             Lost          0
```

Node ID
Indica el ID de nodo del Nuera del puerto de voz.

Absolute Port Address
Indica el identificador del puerto de voz del 2212 utilizado por la contabilidad de llamadas del F200. El software del 2212 genera automáticamente la dirección y es exclusiva para cada puerto de voz de un determinado 2212.

Vocoder Suite
Indica la suite del vocoder (ITU o NUERA) disponible actualmente en el puerto de voz.

Vocoder Rate
Indica la cadencia actual del vocoder.

Vocoder Packet Size
Indica el número de bytes de cada paquete del vocoder. Éste es el tamaño de la salida de compresión en bruto y no incluye la cabecera Frame Relay.

Vocoder Frame Size
Indica el número de muestras PCM de cada trama de vocoder.

Echo Canceller
Indica el estado actual del cancelador de eco.

FAX Demodulation
Indica el estado actual de desmodulación de FAX. El estado puede ser Activo o Desocupado.

FAX Modulation
Indica el estado actual de modulación de FAX. El estado puede ser Activo o Desocupado.

FAX Type
Indica el tipo de modulación que se está utilizando.

FAX Last FCF
Indica el último campo de control de FAX desmodulado.

Last Received Dial Sequence
Indica la última secuencia de dígitos de marcación recibida del abonado a través de la interfaz telco.

Last Received Dial Sequence
Indica la última secuencia de dígitos de marcación enviada al abonado a través de la interfaz telco.

Transmit Packets/ Receive Packets
Muestra información sobre los paquetes Frame Relay transmitidos y recibidos. Los paquetes transmitidos son los paquetes generados por el puerto de voz y enviados a través del enlace Frame Relay. Los paquetes recibidos son los paquetes recibidos por el puerto de voz a través del enlace Frame Relay.

Total Indica el número total de paquetes recibidos y transmitidos.

Voice Indica el número de paquetes de voz comprimidos recibidos y transmitidos.

CAS Indica el número de paquetes CAS recibidos y transmitidos.

DTMF Indica el número de paquetes DTMF recibidos y transmitidos.

FAX Indica el número de paquetes FAX recibidos y transmitidos.

Lost Muestra el número de paquetes enviados por el nodo local pero que no ha recibido el nodo remoto (paquetes transmitidos) y el número de paquetes enviados por el nodo remoto pero que no ha recibido el nodo local (paquetes recibidos).

Trace Call

Utilice el mandato **trace call** para rastrear todos los mensajes de establecimiento o los mandatos de control de configuración de la interfaz de destino. Los sucesos de rastreo pueden verse con el mandato ELS (talk 2).

Sintaxis:

trace call

Apéndice A. Atributos de la seguridad AAA remota

En este apartado se describen los atributos de la seguridad AAA remota que utilizan los servidores Radius, TACACS y TACACS+.

Radius

ID de proveedor de IBM: 211

Atributos de autorización

Del 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 de caracteres
	dirección ip	

Específicos del proveedor de IBM

NAS_TUNNEL_PASSWORD	101
CALLBACK_FLAGS	210
ENCRYPTION	211
HOSTNAME	213
SUBNETMASK	215
PRIVILEGE	216

Palabras clave

Los servidores Radius que permiten la entrada de campos específicos del proveedor utilizan palabras clave `<palabra-clave>=<valor>`.

KWD_CALLBACK_FLAGS	CBF
KWD_ENCRYPTION	ENC
KWD_HOSTNAME	HSN
KWD_SUBNETMASK	SNM
KWD_PRIVILEGE	PRV

Valores

PRIVILEGE:
ADMIN
OPER
MONITOR

CALLBACKFLAGS

REQ	devolución de llamada obligatoria
ROAM	devolución de 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
- elasped_time
- timezone
- event
- reason
- bytes
- bytes_in
- bytes_out
- paks
- paks_in
- paks_out
- status
- err_msg

Apéndice B. Lista de Abreviaturas

AARP protocolo de resolución de direcciones de AppleTalk (AppleTalk Address Resolution Protocol)

ABR direccionador limítrofe de área (area border router)

ack acuse de recibo (acknowledgment)

AIX Advanced Interactive Executive

AMA direccionamiento MAC arbitrario (arbitrary MAC addressing)

AMP supervisor activo presente (active monitor present)

ANSI American National Standards Institute

AP2 Fase 2 de AppleTalk (AppleTalk Phase 2)

APPN comunicaciones avanzadas de igual a igual (Advanced Peer-to-Peer Networking)

ARE explorador de todas las rutas (all-routes explorer)

ARI/FCI
indicador de dirección reconocida/indicador de trama copiada (address recognized indicator/frame copied indicator)

ARP protocolo de resolución de direcciones (Address Resolution Protocol)

AS sistema autónomo (autonomous system)

ASBR direccionador limítrofe de sistema autónomo (autonomous system boundary router)

ASCII código estándar americano para el intercambio de información (American National Standard Code for Information Interchange)

ASN.1 notación de sintaxis abstracta 1 (abstract syntax notation 1)

ASRT direccionamiento en origen adaptativo transparente (adaptive source routing transparent)

ASYNC
asíncrono (asynchronous)

ATCP protocolo de control de AppleTalk (AppleTalk Control Protocol)

ATP protocolo de transacciones de AppleTalk (AppleTalk Transaction Protocol)

AUI interfaz de unidad de conexión (attachment unit interface)

ayt está usted ahí (are you there)

BAN nodo de acceso limítrofe (Boundary Access Node)

BBCM gestor de difusión general de puenteo (Bridging Broadcast Manager)

BECN notificación explícita de congestión hacia atrás (backward explicit congestion notification)

BGP protocolo de pasarela limítrofe (Border Gateway Protocol)

BNC bayonet Niell-Concelman

BNCP protocolo de control de red de puenteo (Bridging Network Control Protocol)

BOOTP
protocolo BOOT (BOOT protocol)

BPDU unidad de datos de protocolo de puente (bridge protocol data unit)

bps bits por segundo

BR puenteo / direccionamiento (bridging / routing)

BRS reserva de ancho de banda (bandwidth reservation)

BSD distribución de software de Berkeley (Berkeley software distribution)

BTP agente de retransmisión de protocolo BOOT (BOOTP relay agent)

BTU unidad de transmisión básica (basic transmission unit)

CAM memoria direccionable por contenido (content-addressable memory)

CCITT
Comité Consultivo Internacional de Telegrafía y Telefonía (Consultative Committee on International Telegraph and Telephone)

CD detección de colisión (collision detection)

CGWCON
consola de pasarela (Gateway Console)

CIDR direccionamiento interdominio sin clases (Classless Inter-Domain Routing)

CIP IP clásico (Classical IP)

CIR velocidad de información comprometida (committed information rate)

CLNP protocolo de red en modalidad sin conexiones (Connectionless-Mode Network Protocol)

CPU unidad central de proceso (central processing unit)

CRC comprobación de redundancia cíclica (cyclic redundancy check)

CRS servidor de informes de configuración (configuration report server)

CTS preparado para transmitir (clear to send)

CUD datos de usuario de llamada (call user data)

DAF filtrado de dirección destino (destination address filtering)

DB base de datos (database)

DBsum
resumen de base de datos (database summary)

DCD detector de señal de línea recibida de canal de datos (data channel received line signal detector)

DCE equipo de terminación de circuito de datos (data circuit-terminating equipment)

DCS servidor conectado directamente (Directly connected server)

DDLC controlador de enlace de datos dual (dual data-link controller)

DDN red de datos de defensa (Defense Data Network)

DDP protocolo de entrega de datagramas (Datagram Delivery Protocol)

DDT herramienta de depuración dinámica (Dynamic Debugging Tool)

DHCP protocolo de configuración dinámica de sistema principal (Dynamic Host Configuration Protocol)

dir conectado directamente (directly connected)

DL enlace de datos (data link)

DLC control de enlace de datos (data link control)

DLCI identificador de conexión de enlace de datos (data link connection identifier)

DLS conmutación de enlace de datos (data link switching)

DLSw conmutación de enlace de datos (data link switching)

DMA acceso de memoria directo (direct memory access)

DNA arquitectura de red digital (Digital Network Architecture)

DNCP protocolo de control de protocolo DECnet (DECnet Protocol Control Protocol)

DNIC código identificador de red de datos (Data Network Identifier Code)

DoD Departamento de Defensa (Department of Defense)

DOS sistema operativo en disco (Disk Operating System)

DR direccionador designado (designated router)

DRAM memoria de acceso aleatorio dinámico (Dynamic Random Access Memory)

DSAP punto de acceso a servicio destino (destination service access point)

DSE equipo de conmutación de datos (data switching equipment)

DSE equipo de conmutación de datos (data switching exchange)

DSR aparato de datos preparado (data set ready)

DSU unidad de servicio de datos (data service unit)

DTE equipo terminal de datos (data terminal equipment)

DTR terminal de datos preparado (data terminal ready)

Dtype tipo de destino (destination type)

DVMRP protocolo de direccionamiento multidifusión por vector de distancia (Distance Vector Multicast Routing Protocol)

E1 velocidad de transmisión de 2,048 Mbps

EDEL delimitador final (end delimiter)

EDI indicador de error detectado (error detected indicator)

EGP protocolo de pasarela exterior (Exterior Gateway Protocol)

EIA Asociación de Industrias de Electrónica (Electronics Industries Association)

ELAN LAN emulada (Emulated LAN)

ELAP protocolo de acceso de enlace EtherTalk (EtherTalk Link Access Protocol)

ELS sistema de anotaciones de sucesos (Event Logging System)

ELSCon consola ELS secundaria (Secondary ELS Console)

ESI identificador de sistema final (End system identifier)

EST Horario Estándar del Este de EEUU (Eastern Standard Time)

Eth Ethernet

fa-ga dirección funcional-dirección de grupo (functional address-group address)

FCS secuencia de comprobación de trama (frame check sequence)

FECN notificación explícita de congestión hacia delante (forward explicit congestion notification)

FIFO primero en entrar, primero en salir (first in, first out)

FLT biblioteca de filtros (filter library)

FR Frame Relay

FRL Frame Relay

FTP protocolo de transferencia de archivos (File Transfer Protocol)

GMT Hora Media de Greeenwich (Greenwich Mean Time)

GOSIP
perfil de interconexión de sistemas abiertos del gobierno (Government Open Systems Interconnection Profile)

GTE Compañía General Telefónica (General Telephone Company)

GWCON
consola de pasarela (Gateway Console)

HDLC control de enlace de datos de alto nivel (high-level data link control)

HEX hexadecimal

HPR direccionamiento de alto rendimiento (high-performance routing)

HST servicios de sistema principal TCP/IP (TCP/IP host services)

HTF formato de tabla de sistemas principales (host table format)

IBD dispositivo de arranque integrado (Integrated Boot Device)

ICMP protocolo de mensajes de control de Internet (Internet Control Message Protocol)

ICP protocolo de control de Internet (Internet Control Protocol)

ID identificación

IDP parte de dominio inicial (Initial Domain Part)

IDP protocolo de datagrama de Internet (Internet Datagram Protocol)

IEEE Instituto de Ingenieros de Electricidad y Electrónica (Institute of Electrical and Electronics Engineers)

Ifc# número de interfaz (interface number)

IGP protocolo de pasarela interior (interior gateway protocol)

InARP
protocolo de resolución inversa de direcciones (Inverse Address Resolution Protocol)

IP protocolo Internet (Internet Protocol)

IPCP protocolo de control de IP (IP Control Protocol)

IPPN red de protocolo IP (IP Protocol Network)

IPX intercambio de paquetes interredes (Internetwork Packet Exchange)

IPXCP protocolo de control de IPX (IPX Control Protocol)

RDSI (ISDN)
Red Digital de Servicios Integrados (integrated services digital network)

ISO Organización Internacional para la Normalización (International Organization for Standardization)

Kbps kilobits por segundo

LAN red de área local (local area network)

LAPB protocolo de acceso de enlace equilibrado (link access protocol-balanced)

LAT transporte de área local (local area transport)

LCS estación de canal de LAN (LAN Channel Station)

LCP protocolo de control de enlace (Link Control Protocol)

LED diodo fotoemisor (light-emitting diode)

LF trama de mayor tamaño (largest frame); salto de línea (line feed)

LIS subred de IP lógica (Logical IP subnet)

LLC control de enlace lógico (logical link control)

LLC2 control de enlace lógico 2 (logical link control 2)

LMI interfaz de gestión local (local management interface)

LRM mecanismo de información de LAN (LAN reporting mechanism)

LS estado de enlace (link state)

LSA anuncio de estado de enlace (link state advertisement)

LSA arquitectura de servicios de enlace (Link Services Architecture)

LSB el bit menos significativo (least significant bit)

LSI interfaz de accesos directos de LAN (LAN shortcuts interface)

LSreq petición de estado de enlace (link state request)

LSrxl lista de retransmisión de estado de enlace (link state retransmission list)

LU unidad lógica (logical unit)

MAC control de acceso al medio (medium access control)

Mb megabit

MB megabyte

Mbps megabits por segundo

MBps megabytes por segundo

MC multidifusión (multicast)

MCF filtrado MAC (MAC filtering)

MIB base de información de gestión (Management Information Base)

MIB II
base de información de gestión II (Management Information Base II)

MILNET
red militar (military network)

MOS sistema operativo de microsistemas (Micro Operating System)

MOSDBG
herramienta de depuración de sistema operativo de microsistemas (Micro Operating System Debugging Tool)

MOSPF
abrir primero la vía más corta con extensiones multidifundidas (Open Shortest Path First with multicast extensions)

MPC canal multivía (Multi-Path Channel)

MPC+ canal multivía para transferencia de datos de alto rendimiento (High performance data transfer (HPDT) Multi-Path Channel)

MSB el bit más significativo (most significant bit)

MSDU
unidad de datos de servicio MAC (MAC service data unit)

MRU unidad de recepción máxima (maximum receive unit)

MTU unidad de transmisión máxima (maximum transmission unit)

nak sin acuse de recibo (not acknowledged)

NAS estación de administración de conmutador Nways (Nways Switch Administration station)

NBMA
acceso múltiple no de difusión general (Non-Broadcast Multiple Access)

NBP protocolo de enlace de nombre (Name Binding Protocol)

NBR contiguo (neighbor)

NCP protocolo de control de red (Network Control Protocol)

NCP protocolo central de red (Network Core Protocol)

NDPS conmutación de vía no disruptiva (non-disruptive path switching)

NetBIOS
sistema básico de entrada/salida de red (Network Basic Input/Output System)

NHRP protocolo de resolución de salto siguiente (Next Hop Resolution Protocol)

NIST Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology)

NPDU unidad de datos de protocolo de red (Network Protocol Data Unit)

NRZ sin retorno a cero (non-return-to-zero)

NRZI inversión sin retorno a cero (non-return-to-zero inverted)

NSAP punto de acceso a servicio de red (Network Service Access Point)

NSF National Science Foundation

NSFNET
National Science Foundation NETwork

NVCNFG
configuración no volátil (nonvolatile configuration)

OPCON
consola de operador (Operator Console)

OSI interconexión de sistemas abiertos (open systems interconnection)

OSICP
protocolo de control de OSI (OSI Control Protocol)

OSPF abrir primero la vía más corta (Open Shortest Path First)

OUI identificador exclusivo de organización (organization unique identifier)

PC sistema personal (personal computer)

PCR velocidad de celdas en punto más alto (peak cell rate)

PDN red de datos pública (public data network)

PING sonda de paquetes InterNet (Packet internet groper)

PDU unidad de datos de protocolo (protocol data unit)

PID identificación de proceso (process identification)

P-P punto a punto (Point-to-Point)

PPP protocolo punto a punto (Point-to-Point Protocol)

PROM
memoria programable de sólo lectura (programmable read-only memory)

PU unidad física (physical unit)

PVC circuito virtual permanente (permanent virtual circuit)

RAM memoria de acceso aleatorio (random access memory)

RD descriptor de ruta (route descriptor)

REM supervisor de errores de llamada (ring error monitor)

REV recepción (receive)

RFC Petición de comentarios (Request for Comments)

RI indicador de llamada; información de direccionamiento (ring indicator; routing information)

RIF campo de información de direccionamiento (routing information field)

RII indicador de información de direccionamiento (routing information indicator)

RIP protocolo de información de direccionamiento (Routing Information Protocol)

RISC sistema de conjunto reducido de instrucciones (reduced instruction-set computer)

RNR recepción no preparada (receive not ready)

ROM memoria de sólo lectura (read-only memory)

ROpcon consola remota de operador (Remote Operator Console)

RPS servidor de parámetros de llamada (ring parameter server)

RTMP protocolo de mantenimiento de tabla de direccionamiento (Routing Table Maintenance Protocol)

RTP protocolo de actualización de direccionamiento (RouTing update Protocol)

RTS petición de emisión (request to send)

Rtype tipo de ruta (route type)

rxmits retransmisiones (retransmissions)

rxmt retransmitir (retransmit)

s segundo

SAF filtrado de dirección origen (source address filtering)

SAP punto de acceso a servicio (service access point)

SAP protocolo de anuncio de servicios (Service Advertising Protocol)

SCR velocidad de celda sostenida (Sustained cell rate)

SCSP protocolo de sincronización de antememoria de servidor (Server Cache Synchronization Protocol)

sdel delimitador inicial (start delimiter)

SDLC retransmisión SDLC, control síncrono de enlace de datos (SDLC relay, synchronous data link control)

seqno número de secuencia (sequence number)

SGID ID de grupo de servidor (sever group id)

SGMP protocolo simple de supervisión de pasarela (Simple Gateway Monitoring Protocol)

SL línea serie (serial line)

SMP supervisor en espera presente (standby monitor present)

SMTP protocolo simple de transferencia de correo (Simple Mail Transfer Protocol)

SNA arquitectura de red de sistemas (Systems Network Architecture)

SNAP protocolo de acceso de subred (Subnetwork Access Protocol)

SNMP protocolo simple de gestión de red (Simple Network Management Protocol)

SNPA punto de conexión de subred (subnetwork point of attachment)

SPF ruta intra-área OSPF (OSPF intra-area route)

SPE1 ruta externa OSPF de tipo 1 (OSPF external route type 1)

SPE2 ruta externa OSPF de tipo 2 (OSPF external route type 2)

SPIA tipo de ruta inter-área OSPF (OSPF inter-area route type)

SPID ID de perfil de servicio (service profile ID)

SPX intercambio de paquetes en secuencia (Sequenced Packet Exchange)

SQE error de calidad de señal (signal quality error)

SRAM memoria estática de acceso aleatorio (static random access memory)

SRB puente de direccionamiento en origen (source routing bridge)

SRF trama direccionada específicamente (specifically routed frame)

SRLY retransmisión SDLC (SDLC relay)

SRT direccionamiento en origen transparente (source routing transparent)

SR-TB puente transparente de direccionamiento en origen (source routing-transparent bridge)

STA estático (static)

STB puente de árbol de extensión (spanning tree bridge)

STE explorador de árbol de extensión (spanning tree explorer)

STP par trenzado apantallado (shielded twisted pair); protocolo de árbol de extensión (spanning tree protocol)

SVC circuito virtual conmutado (switched virtual circuit)

TB puente transparente (transparent bridge)

TCN notificación de cambio de topología (topology change notification)

TCP protocolo de control de transmisión (Transmission Control Protocol)

TCP/IP protocolo de control de transmisión / protocolo Internet (Transmission Control Protocol / Internet Protocol)

TEI identificador de punto de terminal (terminal point identifier)

TFTP protocolo trivial de transferencia de archivos (Trivial File Transfer Protocol)

TKR red en anillo (token ring)

TMO tiempo excedido (timeout)

TOS tipo de servicio (type of service)

TSF tramas de extensión transparente (transparent spanning frames)

TTL tiempo de vida (time to live)

TTY teleescritor (teletypewriter)

TX transmitir (transmit)

UA acuse de recibo no numerado (unnumbered acknowledgment)

UDP protocolo de datagrama de usuario (User Datagram Protocol)

UI información no numerada (unnumbered information)

UTP par trenzado sin apantallar (unshielded twisted pair)

VCC conexión de canal virtual (Virtual Channel Connection)

VINES
VIrtual NEtworking System

VIR velocidad de información variable (variable information rate)

VL enlace virtual (virtual link)

VNI interfaz de red virtual (Virtual Network Interface)

VR ruta virtual (virtual route)

WAN red de área amplia (wide area network)

WRS restauración/redirección de WAN (WAN restoral/reroute)

X.25 redes de paquetes conmutados (packet-switched networks)

X.251 capa física de X.25 (X.25 physical layer)

X.252 capa de tramas de X.25 (X.25 frame layer)

X.253 capa de paquetes de X.25 (X.25 packet layer)

XID identificación de intercambio (exchange identification)

XNS Xerox Network Systems

XSUM suma de comprobación (checksum)

ZIP protocolo de información territorial (Zone Information Protocol) de AppleTalk

ZIP2 protocolo 2 de información territorial (Zone Information Protocol 2) de AppleTalk

ZIT tabla de información territorial (Zone Information Table)

Glosario

Este glosario incluye términos y definiciones de:

- *American National Standard Dictionary for Information Systems*, ANSI X3.172-1990, copyright 1990 de American National Standards Institute (ANSI). Pueden adquirirse copias en American National Standards Institute, 11 West 42nd Street, New York, New York 10036. Las definiciones se identifican mediante el símbolo (A) a continuación de la definición.
- Estándar ANSI/EIA—440-A, *Fiber Optic Terminology* Pueden adquirirse copias en Electronic Industries Association, 2001 Pennsylvania Avenue, N.W., Washington, DC 20006. Las definiciones se identifican mediante el símbolo (E) a continuación de la definición.
- *Information Technology Vocabulary*, desarrollado por el Subcomité 1, Joint Technical Committee 1, de la Organización Internacional para la Normalización y la Comisión Internacional de Electrotécnica (ISO/IEC JTC1/SC1). Las definiciones de las partes publicadas de este vocabulario se identifican mediante el símbolo (I) después de la definición; las definiciones tomadas de los estándares internacionales de borradores, de los borradores de comité y de los papeles de trabajo desarrollados por ISO/IEC JTC1/SC1 se identifican mediante el símbolo (T) después de la definición, que indica que los Cuerpos Nacionales de SC1 participantes no han llegado a un acuerdo final.
- *IBM Dictionary of Computing*, New York: McGraw-Hill, 1994.
- Petición de comentarios Internet: 1208, *Glosario de términos de redes*
- Petición de comentarios Internet: 1392, *Glosario de los usuarios de Internet*
- *Object-Oriented Interface Design: IBM Common User Access Guidelines*, Carmel, Indiana: Que, 1992.

En este glosario se utilizan las siguientes referencias cruzadas:

Contrástese con: Se refiere a un término que tiene un significado opuesto o sustancialmente distinto.

Sinónimo de: Indica que el término tiene el mismo significado que el de un término preferido, definido en el glosario en el lugar que le corresponde.

Sinónimo con: Es una referencia anterior que un término definido hace a todos los demás términos cuyo significado sea equivalente.

Véase: Remite al lector a términos de varias palabras que tienen la primera palabra en común.

Véase también: Remite al lector a términos que tienen un significado relacionado sin ser sinónimos.

A

abrir primero la vía más corta (Open Shortest Path First) (OSPF). En la serie de protocolos de Internet, función que proporciona transferencia de información intradominio. Como alternativa del protocolo RIP (protocolo de información de direccionamiento), OSPF permite el direccionamiento de coste más bajo y maneja el direccionamiento en las redes regionales o corporativas de gran tamaño.

accesibilidad (reachability). Capacidad de un nodo o un recurso para comunicarse con otro nodo u otro recurso.

acceso de memoria directo (direct memory access) (DMA). Recurso del sistema que permite a un dispositivo del bus Micro Channel acceder directamente a la memoria del sistema o de bus sin la intervención del procesador del sistema.

acceso múltiple con detección de portadora y detección de colisión (carrier sense multiple access with collision detection) (CSMA/CD). Protocolo que requiere la detección de portadora y en el que una estación de datos en transmisión que detecte otra señal durante la transmisión, detenga el envío, envíe una señal de interferencia y luego espere durante un tiempo variable antes de volver a intentarlo. (T) (A)

ACCESS. En el protocolo simple de gestión de red (SNMP), la cláusula de un módulo MIB (base de información de gestión) que define el nivel de soporte mínimo que un nodo gestionado proporciona en relación a un objeto.

activo (active). (1) Operativo. (2) Dícese del nodo o dispositivo que está conectado o disponible para conectarse a otro nodo o dispositivo.

actualización la de base de datos de topología (topology database update) (TDU). Mensaje acerca de un nodo o un enlace nuevo o cambiado que se difunde entre los nodos de red APPN para mantener la base de datos de topología de red, la cual está totalmente reproducida en cada uno de los nodos. Una TDU contiene información que identifica los elementos siguientes:

- El nodo emisor
- Las características de nodo y enlace de los diversos recursos de la red
- El número de secuencia de la actualización más reciente de cada uno de los recursos descritos.

acuse de recibo (acknowledgment). (1) Transmisión, por parte de un destinatario, de caracteres de acuse de recibo como respuesta afirmativa a un remitente. (T)

(2) Indicación de que se ha recibido un elemento enviado.

Agencia Operante Privada Reconocida (Recognized Private Operating Agency) (RPOA). Cualquier individuo, compañía o corporación, distinto de un departamento o un servicio del gobierno, que dirija un servicio de telecomunicaciones y esté sujeto a las obligaciones comprometidas en el Convenio de la Unión Internacional de Telecomunicaciones y en los Reglamentos; por ejemplo, una empresa de telecomunicación.

agente (agent). Sistema que desempeña el cometido de agente.

alerta (alert). 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 que consta de productores, consumidores y grupos de interés general y que establece los procedimientos por los cuales organizaciones acreditadas crean y mantienen voluntariamente los estándares de la industria en los Estados Unidos. (A)

analógico (analog). (1) Dícese de los datos que constan de cantidades físicas continuamente variables. (A) (2) Contrástese con *digital*.

ancho de banda (Bandwidth). El ancho de banda de un enlace óptico designa la capacidad de transporte de información del enlace y está relacionado con la velocidad máxima de bit que puede admitir un enlace de fibra.

anillo (ring). Véase *red anular*.

anomalía de autenticación (authentication failure). En el protocolo simple de gestión de red (SNMP), captura de excepción que una entidad de autenticación puede haber generado cuando un cliente solicitante no es miembro de la comunidad SNMP.

antememoria - poner en antememoria; (cache). (1) Almacenamiento intermedio de uso especial, más pequeño y rápido que el almacenamiento principal, que permite mantener una copia de instrucciones y datos obtenidos a partir del almacenamiento principal y que es probable que el procesador vaya a necesitar a continuación. (T) (2) Almacenamiento intermedio que contiene instrucciones y datos utilizados con frecuencia; permite reducir el tiempo de acceso. (3) Parte opcional de la base de datos de directorio de una red de nodos en la que puede almacenarse información de directorio utilizada con frecuencia para, así, agilizar las búsquedas en directorio. (4) Colocar, ocultar o almacenar en una antememoria.

aparato de datos preparado (data set ready) (DSR). Sinónimo de *DCE preparado*.

AppleTalk. Protocolo de red desarrollado por Apple Computer, Inc. Se utiliza para interconectar dispositivos de red, que pueden ser una mezcla de productos Apple y no Apple.

árbol de extensión (spanning tree). En los contextos de LAN, método por el que los puentes desarrollan automáticamente una tabla de direccionamiento y la actualizan como respuesta a la topología cambiante para garantizar que sólo haya una ruta entre dos LAN de la red puenteada. Este método evita que se produzcan bucles de paquetes, en los que un paquete circula por una ruta sinuosa para volver al direccionador que lo emitió.

archivo de configuración (configuration file). Archivo que especifica las características de un dispositivo del sistema o de una red.

área (area). En los protocolos de direccionamiento Internet y DECnet, subconjunto de una red o de una pasarela creado por definición del administrador de la red. Las áreas se autocontienen; el conocimiento de la topología de un área permanece oculto para las demás áreas.

arquitectura de interconexión de sistemas abiertos (Open Systems Interconnection (OSI) architecture). Arquitectura de red que se ajusta a un conjunto concreto de estándares ISO en relación a la interconexión de sistemas abiertos. (T)

arquitectura de red (network architecture). Estructura lógica y principios operativos de una red de sistemas. (T)

Nota: Los principios operativos de una red incluyen los de los servicios, funciones y protocolos.

arquitectura de red de sistemas (Systems Network Architecture) (SNA). Descripción de la estructura lógica, formatos, protocolos y secuencias operativas que permiten transmitir unidades de información a través de las redes, así como controlar la configuración y el funcionamiento de éstas. La estructura por capas de SNA permite a los orígenes y destinos últimos de la información, es decir, a los usuarios, ser independientes y no verse afectados por los servicios y los recursos de red SNA específicos utilizados para el intercambio de la información.

arquitectura de red digital (Digital Network Architecture) (DNA). Modelo de todas las implementaciones de hardware y software de DECnet.

arreglo temporal del programa (program temporary fix) (PTF). Solución temporal o manera de eludir un problema diagnosticado por IBM en un release actual e inalterable del programa.

asíncrono (asynchronous) (ASYNC). Dícese de dos o más procesos que no dependen de que se produzcan sucesos específicos, tales como señales de sincronización común. (T)

B

base de datos de configuración (configuration database) (CDB). Base de datos en la que se almacenan los parámetros de configuración de uno o varios dispositivos. Se prepara y actualiza utilizando el programa de configuración.

base de información de gestión (Management Information Base) (MIB). (1) Conjunto de objetos a los que se puede acceder por medio de un protocolo de gestión de red. (2) Definición de la información de gestión que especifica la información disponible en un sistema principal o en una pasarela y las operaciones que están permitidas. (3) En OSI, depósito conceptual de la información de gestión dentro de un sistema abierto.

baudio (baud). En la transmisión asíncrona, unidad de frecuencia de modulación en correspondencia con un intervalo unidad por segundo; por ejemplo, si la duración del intervalo unidad es de 20 milisegundos, la frecuencia de modulación sería igual a 50 baudios. (A)

bit D (D-bit). Bit de confirmación de entrega. En las comunicaciones X.25, bit de un paquete de datos o de un paquete de petición de llamada que se establece en 1 si el destinatario requiere acuse de recibo entre extremos (confirmación de entrega).

bucle de direccionamiento (routing loop). Situación que acontece cuando los direccionadores hacen circular información entre ellos mismos hasta que se produce una convergencia o hasta que las redes implicadas se consideran inaccesibles.

C

cabecera (header). (1) Información de control definida por el sistema y que precede a los datos de usuario. (2) Parte de un mensaje que contiene información de control correspondiente al mensaje, como por ejemplo, uno o más campos del destino, el nombre de la estación origen, el número de secuencia de entrada, una serie de caracteres que indique el tipo de mensaje y el nivel de prioridad del mensaje.

cabecera de transmisión (transmission header) (TH). Información de control, seguida opcionalmente por una unidad de información básica (BIU) o un segmento de BIU, creada y utilizada por el control de vía para direccionar las unidades de mensaje y controlar el flujo de estas unidades en la red. Véase también *unidad de información de vía*.

canal (channel). (1) Vía por la que pueden enviarse señales como, por ejemplo, el canal de datos, el 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 periférico local.

canal de entrada/salida (input/output channel). En un sistema de proceso de datos, unidad funcional que maneja la transferencia de datos entre el equipo interno y el periférico. (I) (A)

canal lógico (logical channel). En las operaciones en modalidad de paquetes, canal emisor y canal receptor que se utilizan juntos y simultáneamente para enviar y recibir datos a través de un enlace de datos. Pueden establecerse varios canales lógicos en un mismo enlace de datos interponiendo la transmisión de paquetes.

canal multivía (multipath channel) (MPC). Protocolo de canal que utiliza múltiples canales monodireccionales para la comunicación bidireccional VTAM con VTAM.

canalización (channelization). Proceso de dividir el ancho de banda de una línea de comunicaciones en un número determinado de canales, posiblemente de distinto tamaño. También se llama ***multiplexado por división de tiempo*** (TDM).

capa (layer). (1) En la arquitectura de redes, grupo de servicios que puede considerarse completo desde el punto de vista conceptual, que forma parte de un conjunto de grupos organizados jerárquicamente y que se extiende a todos los sistemas que constituyen la arquitectura de la red. (T) (2) En el modelo de referencia OSI (interconexión de sistemas abiertos), uno de los siete grupos de servicios, funciones y protocolos considerados conceptualmente completos, organizados jerárquicamente y que se extienden a todos los sistemas abiertos. (T) (3) En SNA, agrupación de funciones relacionadas, separadas lógicamente de las funciones de los demás grupos. Puede cambiarse la implementación de las funciones de una capa sin que por ello se vean afectadas las funciones de las otras capas.

capa (layer) de control de enlace de datos (DLC). En SNA, capa que consta de las estaciones de enlace que planifican la transferencia de datos a través de un enlace entre dos nodos y llevan a cabo el control de errores para el enlace. Ejemplos de control de enlace de datos son SDLC para la conexión de enlace serie por bit y el control de enlace de datos para el canal de System/370.

Nota: La capa DLC suele ser independiente del mecanismo de transporte físico y garantiza la integridad de los datos que acceden a las capas más altas.

capa de enlace de datos (data link layer). En el modelo de referencia de la interconexión de sistemas abiertos (Open Systems Interconnection), capa que proporciona los servicios de transferencia de datos entre las entidades de la capa de red a lo largo de un enlace de comunicaciones. La capa de enlace de datos detecta y, posiblemente, corrige los errores que puedan producirse en la capa física. (T)

capa de red (network layer). En la arquitectura OSI (interconexión de sistemas abiertos), capa responsable de direccionar, conmutar y enlazar el acceso a las capas en el entorno OSI.

capa de transporte (transport layer). En el modelo de referencia de la interconexión de sistemas abiertos (Open Systems Interconnection), capa que proporciona un servicio de transferencia de datos fiable de extremo a extremo. En la vía puede haber sistemas abiertos de retransmisión. (T) Véase también *modelo de referencia de interconexión de sistemas abiertos*.

capa física (physical layer). En el modelo de referencia OSI (interconexión de sistemas abiertos), capa que proporciona los medios mecánicos, eléctricos, funcionales y procedimentales para establecer, mantener y liberar conexiones físicas a través del medio de transmisión. (T)

captura de excepción (trap). En el protocolo simple de gestión de red (SNMP), mensaje enviado por un nodo gestionado (función de agente) a una estación de gestión para informar de una condición de excepción.

carácter coincidente con patrón (pattern-matching character). Carácter especial, como puede ser un asterisco (*) o un signo de interrogación (?) que puede utilizarse para representar uno o varios caracteres. Cualquier carácter o conjunto de caracteres puede sustituir a un carácter coincidente con patrón. Sinónimo con *carácter global* y *carácter comodín*.

carácter comodín (wildcard character). Sinónimo de *carácter coincidente con patrón*.

CCITT. Comité Consultivo Internacional de Telegrafía y Telefonía (International Telegraph and Telephone Consultative Committee). Formaba parte de la Unión Internacional de Telecomunicaciones (ITU). El día 1 de marzo de 1993, se reorganizó ITU, y las responsabilidades correspondientes a la normalización se pusieron a cargo de una organización subordinada que se llamaba Sector para la Normalización de Telecomunicaciones de la Unión de Telecomunicaciones (ITU-TS). "CCITT" sigue utilizándose para las recomendaciones que se aprobaron antes de la reorganización.

central telefónica privada (private branch exchange) (PBX). Central telefónica de uso privado que permite transmitir llamadas a y desde una red telefónica pública.

centralita de red digital integrada (Integrated Digital Network Exchange) (IDNX). Procesador que integra aplicaciones de voz, datos e imagen. También gestiona los recursos de transmisión y se conecta a multiplexadores y a sistemas de soporte de gestión de redes. Permite la integración de equipos de distintos proveedores.

centro de información de red (Network Information Center) (NIC). En las comunicaciones Internet, grupos locales, regionales y nacionales de todo el mundo que proporcionan a los usuarios ayuda, documentación y capacitación, entre otros servicios.

circuito de datos (data circuit). (1) Par de canales asociados para la transmisión y la recepción, que proporcionan un medio de comunicación de datos bidireccional. (I) (2) En SNA, sinónimo de *conexión de enlace*. (3) Véase también *circuito físico* y *circuito virtual*.

Notas:

1. Entre equipos de conmutación de datos, el circuito de datos puede incluir un equipo de terminación de circuito de datos (DCE), según sea el tipo de interfaz utilizada en el equipo de conmutación de datos.
2. Entre una estación de datos y un equipo de conmutación de datos o un 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 parecido a un DCE en la ubicación del equipo de conmutación de datos o del concentrador de datos.

circuito físico (physical circuit). Circuito establecido sin multiplexación. Véase también *circuito de datos*. Contrástese con *circuito virtual*.

circuito huérfano (orphan circuit). Circuito no configurado cuya disponibilidad se conoce dinámicamente.

circuito virtual (virtual circuit). (1) En conmutación de paquetes, recursos proporcionados por una red que el usuario ve como si fuese una conexión real. (T) Véase también *circuito de datos*. Contrástese con *circuito físico*. (2) Conexión lógica establecida entre dos DTE.

circuito virtual conmutado (switched virtual circuit) (SVC). Circuito X.25 que se establece dinámicamente en cuanto se necesita. Es el equivalente en X.25 de una línea conmutada. Contrástese con *circuito virtual permanente (PVC)*.

circuito virtual permanente (permanent virtual circuit) (PVC). En las comunicaciones X.25 y frame-relay, circuito virtual al que se ha asignado de forma permanente un canal lógico en cada equipo terminal de datos (DTE). No se requieren protocolos de establecimiento de llamada. Contrástese con *circuito virtual conmutado (SVC)*.

clase de productividad (throughput class). En la conmutación de paquetes, velocidad a la que los paquetes del equipo terminal de datos (DTE) viajan a través de la red de conmutación de paquetes.

clase de servicio (class of service) (COS). Conjunto de características (como la seguridad de ruta, la prioridad de transmisión, el ancho de banda) utilizado para construir una ruta entre interlocutores de sesión. La clase de servicio se deriva de un nombre de modalidad especificado por el iniciador de una sesión.

cliente (client). (1) Unidad funcional que recibe servicios compartidos de un servidor. (T) (2) Un usuario.

cliente/servidor (client/server). En comunicaciones, modelo de interacción en el proceso de datos distribuido en el que un programa de un local envía una petición a un programa de otro local y espera una

respuesta. El programa solicitante sería el cliente; el programa que responde, el servidor.

codificar (encode). Transformar los datos mediante un código de tal manera que sea posible devolverles su forma original. (T)

coeficiente de información comprometida (Commited information rate). Cantidad máxima de datos en bits que la red se presta a entregar.

coeficiente de pérdida de paquete (packet loss ratio). Probabilidad de que un paquete no llegue a su destino o de que no llegue al destino antes de un momento especificado.

colisión (collision). Condición no deseable provocada por las transmisiones concurrentes de un canal. (T)

compresión (compression). (1) Proceso de eliminar huecos, campos vacíos, redundancias y datos innecesarios con el fin de acortar la longitud de los registros o de los bloques. (2) Cualquier codificación que permita reducir el número de bits empleados para representar un determinado mensaje o registro.

comunicaciones avanzadas de igual a igual (Advanced Peer-to-Peer Networking) (APPN). Ampliación de SNA que ofrece (a) un mayor control de red distribuida que evite dependencias jerárquicas críticas, aislando así los efectos de los puntos de anomalía individuales; (b) el intercambio dinámico de información de topología de red para favorecer la facilidad de conexión, la reconfiguración y la selección de rutas adaptativa; (c) la definición dinámica de los recursos de red; y (d) el registro de recursos y la búsqueda en directorio automatizados. APPN amplía la orientación igual de LU 6.2 para los servicios de usuario final en el control de red y da soporte a múltiples tipos de LU, entre ellos, a LU 2, LU 3 y LU 6.2.

comunidad (community). En el protocolo simple de gestión de red (SNMP), relación administrativa entre las entidades.

concentrador inteligente (hub). Concentrador de cableado, como puede ser el IBM 8260, que proporciona funciones de puenteo o direccionamiento para las LAN que tienen distintos cables y protocolos.

conectado por enlace (link-attached). (1) Dícese de los dispositivos que están conectados a una unidad de control por un enlace de datos. (2) Contrástese con *conectado por canal*. (3) Sinónimo con *remoto*.

conexión (connection). En la comunicación de datos, asociación establecida entre unidades funcionales para comunicar información. (I) (A)

conexión de enlace (link connection). (1) Equipo físico que proporciona una comunicación bidireccional entre una estación de enlace y otra (u otras) estación de enlace; por ejemplo, una línea de telecomunicaciones y un equipo de terminación de circuito de datos (DCE). (2) En SNA, sinónimo con *circuito de datos*.

conexión de protocolo de transporte rápido (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 (virtual connection). En frame relay, vía de retorno de una conexión potencial.

configuración (configuration). (1) Manera en la que se ha organizado e interconectado el hardware y el software de un sistema de proceso de información. (T) (2) Los dispositivos y los programas que constituyen un sistema, subsistema o red.

configuración del sistema (system configuration). Proceso que especifica los dispositivos y los programas que forman un sistema determinado de proceso de datos.

congestión (congestion). Véase *congestión de red (network congestion)*.

congestión de red (network congestion). Condición no deseable de carga excesiva provocada por un tráfico que supera al que la red es capaz de manejar.

conmutación de circuitos (circuit switching). (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 los DTE hasta que se libere la conexión. (I) (A) (2) Sinónimo con *conmutación de líneas*.

conmutación de enlace de datos (data link switching) (DLSw). Método de transporte de protocolos de red que utilizan el control de enlace lógico (LLC) IEEE 802.2 de tipo 2. SNA y NetBIOS son ejemplos de protocolos que utilizan LLC de tipo 2. Véase también *encapsulación* y *usurpación*.

conmutación de líneas (line switching). Sinónimo de *conmutación de circuitos*.

conmutación de paquetes (packet switching). (1) Proceso de direccionar y transferir datos por medio de paquetes direccionados para que un canal sólo esté ocupado durante la transmisión de un paquete. Una vez completada la transmisión, el canal se vuelve disponible para la transferencia de otros paquetes. (I) (2) Sinónimo con *operación en modalidad de paquetes*. Véase también *conmutación de circuitos*.

Conmutador Nways (Nways Switch). Sinónimo con el conmutador de banda ancha IBM 2220 Nways.

consola remota (remote console). Estación que ejecuta OS/2, TCP/IP y el programa de control de recursos de conmutador Nways. Puede conectarse a cualquier estación de soporte de red para operar y dar servicio de forma remota al conmutador Nways.

La conexión puede establecerse mediante:

- Una línea conmutada que utilice un módem

Cualquier estación de soporte de red que se utilice como consola remota de otra estación de soporte de red.

contigua activa de donde proceden los datos (nearest active upstream neighbor) (NAUN). En la red en anillo de IBM, estación que envía los datos directamente a una determinada estación del anillo.

contiguo (neighbor). Direccionador de una subred común que un administrador de red ha designado para recibir la información de direccionamiento.

control de acceso al medio (medium access control) (MAC). En las LAN, subcapa de la capa de control de enlace de datos que da soporte a funciones dependientes de medio y que 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 que permite determinar cuándo un dispositivo tiene acceso al medio de transmisión.

control de enlace de datos (data link control) (DLC). Conjunto de reglas utilizadas por los nodos en un enlace de datos (por ejemplo, un enlace SDLC o una red en anillo) para lograr un intercambio ordenado de información.

control de enlace de datos de alto nivel (high-level data link control) (HDLC). En la comunicación de datos, uso de series de bits especificadas para controlar enlaces de datos de acuerdo con los estándares internacionales de HDLC: ISO 3309 Estructura de trama e ISO 4335 Elementos de procedimientos.

control de enlace lógico (logical link control) (LLC). Subcapa de LAN de control de enlace de datos (DLC) que proporciona dos tipos de operación de DLC para el intercambio ordenado de datos. El primer tipo es un servicio sin conexiones que permite que la información se envíe y se reciba sin establecer un enlace. La subcapa de LLC no realiza la recuperación de errores ni el control de flujo para el servicio sin conexiones. El segundo tipo es un servicio orientado a conexiones que requiere el establecimiento de un enlace antes del intercambio de información. El servicio orientado a la conexión proporciona la transferencia de información en secuencia, el control de flujo y la recuperación de errores.

control de flujo (flow control). (1) En SNA, proceso de gestionar la velocidad con la que el tráfico de datos pasa entre los componentes de la red. La finalidad del control de flujo es optimizar la velocidad con que fluyen las unidades de mensaje en relación a una congestión mínima de la red; es decir, lograr que los almacenamientos intermedios no queden desbordados en el receptor ni en los nodos de direccionamiento intermedio, y que el receptor no quede a la espera de más unidades de mensaje. (2) Véase también *ritmo*.

control de vía (path control) (PC). Función que direcciona las unidades de mensaje entre las unidades accesibles de la red y proporciona las vías entre ellas. Hace que las unidades de información básica (BIU) del control de transmisión se conviertan (posiblemente, segmentándolas) en unidades de información de vía (PIU) e intercambia las unidades de transmisión básica que contienen uno o varios PIU con el control de enlace de datos. El control de vía varía según el tipo de nodo: algunos nodos (por ejemplo, los nodos APPN) utilizan identificadores de sesión generados localmente para el direccionamiento; otros (los nodos de subárea) utilizan direcciones de red para el direccionamiento.

control síncrono de enlace de datos (Synchronous Data Link Control) (SDLC). (1) Disciplina en conformidad con subconjuntos de ADCCP (procedimientos avanzados de control de comunicación de datos), de American National Standards Institute (ANSI), y HDCL (control de enlace de datos de alto nivel) de la Organización Internacional para la Normalización, que permite gestionar la transferencia de información serie por bit y transparente para código a través de una conexión de enlace. Los intercambios de la transmisión pueden ser dúplex o semi-dúplex a través de enlaces conmutados o no conmutados. La configuración de la conexión de enlace puede ser punto a punto, multipunto o en bucle. (I) (2) Contrástese con *comunicación síncrona en binario (BSC)*.

correlación (mapping). Proceso de hacer que los datos que un remitente transmite con un formato se conviertan al formato de datos que puede aceptar el destinatario.

corriente general de datos (general data stream) (GDS). Corriente de datos utilizada para las conversaciones en las sesiones de LU 6.2.

coste de vía (path cost). En los protocolos de direccionamiento por estado de enlace, suma de los costes de enlace a lo largo de la vía entre dos nodos o redes.

cronometraje (clocking). (1) En la comunicación síncrona en binario, uso de los impulsos de reloj para controlar la sincronización de los caracteres de datos y de control. (2) Método que controla el número de bits de datos enviados en una línea de telecomunicaciones en un momento dado.

cuenta de saltos (hop count). (1) Métrica o medida de la distancia entre dos puntos. (2) En las comunicaciones Internet, número de direccionadores a través de los que pasa un datagrama cuando se dirige a su destino. (3) En SNA, medida del número de enlaces que han de atravesarse en una vía hacia un destino.

D

daemon. Programa que se ejecuta en modalidad desatendida para prestar un servicio estándar. Algunos daemons se desencadenan automáticamente para realizar su tarea; otros se ponen en marcha periódicamente.

datagrama (datagram). (1) En la conmutación de paquetes, paquete autocontenido e independiente de los demás paquetes, que transporta información suficiente para el direccionamiento desde el DTE (equipo terminal de datos) origen al DTE destino sin contar con los intercambios anteriores entre los DTE y la red. (I) (2) En TCP/IP, unidad de información

básica que se pasa en el entorno Internet. Un datagrama contiene una dirección origen y una dirección destino, además de los datos. Un datagrama IP (protocolo Internet) consta de una cabecera IP seguida de los datos de la capa de transporte. (3) Véase también *paquete* y *segmento*.

datagrama IP (IP datagram). En la serie de protocolos de Internet, unidad fundamental de información que se transmite a través de un conjunto de redes. Contiene las direcciones origen y destino, los datos de usuario e información de control tal como la longitud del datagrama, la suma de comprobación de la cabecera, y distintivos que indican si el datagrama puede fragmentarse o ya se ha fragmentado.

DCE preparado (DCE ready). En el estándar 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 comunicación y preparado para enviar datos. Sinónimo de *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 usados típicamente para ligar entre sí sistemas DEC (corporación de equipos digitales) para el compartimiento de recursos, el cálculo distribuido o la configuración de sistemas remotos. Las implementaciones de la red DECnet se ajustan al modelo DNA (arquitectura de red digital).

detección de colisión (collision detection). 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 (carrier sense). En una red de área local, actividad continuada de una estación de datos que permite detectar si hay otra estación que esté transmitiendo. (T)

detector de portadora (carrier detect). Sinónimo de *detector de señal de línea recibida (RLSD)*.

detector de portadora de datos (data carrier detect) (DCD). Sinónimo de *detector de señal de línea recibida (RLSD)*.

detector de señal de línea recibida (received line signal detector) (RLSD). En el estándar 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). Sinónimo con *detector de portadora* y *detector de portadora de datos (DCD)*.

determinación de problemas (problem determination). Proceso de determinar el origen de un problema; por ejemplo, un componente de programa, una avería de máquina, recursos de telecomunicaciones, programas o equipo instalados por el usuario o por el contratista, o una anomalía ambiental tal como un corte en el suministro eléctrico o un error de usuario.

difusión general (broadcast). (1) Transmisión de unos mismos datos a todos los destinos. (T) (2) Transmisión simultánea de datos a más de un destino. (3) Contrástese con *multidifusión*.

digital. (1) Relativo a los datos que constan de dígitos. (T) (2) Relativo a los datos que tienen formato de dígitos. (A) (3) Contrástese con *analógico*.

dirección (address). En la comunicación de datos, código exclusivo asignado a cada dispositivo, estación de trabajo o usuario conectados a una red.

dirección administrada localmente (locally administered address). En una red de área local, dirección de adaptador que el usuario puede asignar para alterar de forma temporal la dirección administrada universalmente. Contrástese con *dirección administrada universalmente*.

dirección administrada universalmente (universally administered address). En una red de área local, dirección codificada de modo permanente en un adaptador en el momento de la fabricación. Todas las direcciones administradas universalmente son exclusivas. Contrástese con *dirección administrada localmente*.

dirección canónica (canonical address). En las LAN, formato IEEE 802.1 de la transmisión de direcciones MAC (control de acceso al medio) para adaptadores de red en anillo y Ethernet. En el formato canónico, se transmite en primer lugar el bit menos significativo (el de más a la derecha) de cada uno de los bytes de la dirección. Contrástese con *dirección no canónica*.

dirección de difusión general (broadcast address). En comunicaciones, dirección de estación (ocho unos) reservada como dirección común a todas las estaciones de un enlace. Sinónimo con *dirección de todas las estaciones*.

dirección de red (network address). Según ISO 7498-3, nombre inequívoco dentro del entorno OSI y que identifica un conjunto de puntos de acceso a los servicios de red.

dirección de subred (subnet address). En las comunicaciones Internet, extensión del esquema básico de direcciones IP en la que una parte de la dirección del sistema principal se interpreta como dirección de red local.

dirección de todas las estaciones (all-stations address). En comunicaciones, sinónimo de *dirección de difusión general*.

dirección de usuario de red (network user address) (NUA). En las comunicaciones X.25, dirección X.121 que contiene como máximo 15 dígitos de código binario.

dirección Internet (Internet address). Véase *dirección IP*.

dirección IP (IP address). Dirección de 32 bits definida por el protocolo Internet, estándar 5, petición

de comentarios (RFC) 791. Suele representarse en notación decimal con puntos.

dirección no canónica (noncanonical address). En las LAN, formato de la transmisión de direcciones MAC (control de acceso al medio) para adaptadores de red en anillo. En el formato no canónico se transmite en primer lugar el bit más significativo (el de más a la izquierda) de cada uno de los bytes de la dirección. Contrástese con *dirección canónica*.

direccionador (router). (1) Sistema informático que determina la vía por la que fluye el tráfico de la red. La selección de vía se realiza a partir de la información, basada en varias vías, que se obtiene de protocolos específicos, algoritmos que intentan identificar cuál es la vía más corta o la mejor, y otros criterios como, por ejemplo, la métrica o las direcciones destino específicas de protocolo. (2) Dispositivo de conexión que conecta dos segmentos de LAN, que utilicen una arquitectura parecida o arquitecturas distintas, en la capa de red del modelo de referencia. (3) En la terminología OSI, función que determina una vía por la que puede accederse a una entidad. (4) En TCP/IP, sinónimo con *pasarela*. (5) Contrástese con *puente*.

direccionador designado (designated router). Direccionador que informa a los nodos finales de la existencia y de la identidad de otros direccionadores. La selección del direccionador designado se basa en el direccionador cuya prioridad sea la más alta. Cuando varios direccionadores comparten la prioridad más alta, se selecciona el direccionador que tenga la dirección de estación más alta.

direccionador germen (seed router). En las redes AppleTalk, direccionador que mantiene los datos de configuración (por ejemplo, los números de rango de red y las listas territoriales) de la red. Cada red debe tener al menos un direccionador germen. El direccionador germen debe configurarse inicialmente utilizando la herramienta configuradora. Contrástese con *direccionador no germen*.

direccionador IP (IP router). Dispositivo de interredes IP que es el responsable de tomar decisiones acerca de las vías por las que va a fluir el tráfico de red. Se utilizan protocolos de direccionamiento para obtener información acerca de la red y para determinar cuál es la mejor ruta por la que conviene enviar el datagrama hacia el destino final. Los datagramas se direccionan basándose en las direcciones IP del destino.

direccionador limítrofe (border router). En comunicaciones Internet, direccionador situado en el borde de un sistema autónomo que se comunica con un direccionador situado en el borde de otro sistema autónomo.

direccionador no germen (nonseed router). En las redes AppleTalk, direccionador que adquiere información de rango de números de red y de lista territorial de un direccionador germen conectado a la misma red.

direccionador troncal (backbone router). (1) Direccionador utilizado para la transmisión de datos entre áreas. (2) Uno de una serie de direccionadores que permite interconectar las redes de un conjunto de redes de mayor tamaño.

direccionamiento (addressing). En la comunicación de datos, manera que una estación tiene de seleccionar la estación a la que va a enviar datos.

direccionamiento (routing). (1) Asignación de la vía por la que un mensaje ha de acceder al destino que le corresponde. (2) En SNA, reenvío de una unidad de mensaje a lo largo de una determinada vía a través de una red, según lo determinen los parámetros transportados en la unidad de mensaje como, por ejemplo, la dirección de red destino de una cabecera de transmisión.

direccionamiento de alto rendimiento (high-performance routing) (HPR). Adición realizada en la arquitectura APPN (comunicaciones avanzadas de igual a igual) que mejora el rendimiento y la fiabilidad del direccionamiento de datos, en especial cuando se utilizan enlaces de alta velocidad.

direccionamiento de sesión intermedia (intermediate session routing) (ISR). Tipo de función de direccionamiento dentro de un nodo de red APPN que proporciona control de flujo a nivel de sesión, e información de indisponibilidad para todas las sesiones que pasan a través del nodo, pero cuyos puntos finales están en otro lugar.

direccionamiento dinámico (Dynamic Routing). Direccionamiento que utiliza rutas aprendidas, en vez de las rutas configuradas estáticamente en la inicialización.

direccionamiento en origen (source routing). En las LAN, método por el que la estación emisora determina la ruta que la trama va a seguir e incluye la información de direccionamiento junto con la trama. Los puentes pueden leer la información de direccionamiento para determinar si tienen que reenviar la trama.

direccionamiento intra-área (intra-area routing). En las comunicaciones Internet, el direccionamiento de datos dentro de un área.

direccionamiento MAC arbitrario (arbitrary MAC addressing) (AMA). En la arquitectura DECnet, esquema de direccionamiento utilizado por DECnet Phase IV-Prime que da soporte a direcciones administradas universalmente y a direcciones administradas localmente.

directorio (directory). Tabla de identificadores y referencias a los correspondientes elementos de datos. (I) (A)

dispositivo (device). Aparato mecánico, eléctrico o electrónico con una finalidad específica.

dominio (domain). (1) Parte de una red de sistemas en la que los recursos de proceso de datos están bajo

control común. (T) (2) En OSI (interconexión de sistemas abiertos), parte de un sistema distribuido o de un conjunto de objetos gestionados a la que se aplica una política común. (3) Véase *dominio administrativo* y *nombre de dominio.*

dominio administrativo (Administrative Domain). Conjunto de sistemas principales y direccionadores, incluidas las redes de interconexión, gestionado por una sola autoridad administrativa.

dominio de direccionamiento (routing domain). En las comunicaciones Internet, grupo de sistemas intermedios que utilizan un protocolo de direccionamiento tal que la representación de la red global sea idéntica dentro de cada uno de los sistemas intermedios. Los dominios de direccionamiento se conectan entre sí mediante enlaces exteriores.

E

eco (echo). En la comunicación de datos, señal reflejada de un canal de comunicación. Por ejemplo, en un terminal de comunicaciones, cada señal se visualiza dos veces: una cuando entra en el terminal local y otra cuando vuelve a través del enlace de comunicaciones. El eco permite comprobar las señales dos veces a efectos de exactitud.

EIA 232. En la comunicación de datos, especificación de EIA (Electronic Industries Association) que define la interfaz entre el equipo terminal de datos (DTE) y el equipo de terminación de circuito de datos (DCE), y que utiliza el intercambio de datos en binario y en serie.

Electronic Industries Association (EIA). Organización de fabricantes de electrónica que promueve el crecimiento tecnológico de la industria, representa las perspectivas de sus miembros y desarrolla los estándares de la industria.

encapsulación (encapsulation). (1) En comunicaciones, técnica utilizada por los protocolos con capas y mediante la que una capa añade información de control a la unidad de datos de protocolo (PDU) de la capa a la que da soporte. Por lo que se refiere a esto, la capa encapsula los datos de la capa soportada. Por ejemplo, en la serie de protocolos de Internet, un paquete contendría la información de control de la capa física, seguida de la información de control de la capa de red, seguida de los datos del protocolo de la aplicación. (2) Véase también *conmutación de enlace de datos.*

enlace (link). 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 se puede compartir entre múltiples enlaces de una configuración multipunto o de red en anillo.

enlace lógico (logical link). Par de estaciones de enlace, una en cada uno de un par de nodos adyacentes, junto con la conexión de enlace subyacente de las mismas, que proporcionan una conexión de una sola capa de enlace entre los dos nodos. Pueden distinguirse múltiples enlaces lógicos mientras comparten el uso de un mismo medio físico que conecta dos nodos. Son ejemplos los enlaces lógicos 802.2 utilizados en los recursos de LAN (red de área local) y los enlaces lógicos E LAP de un mismo enlace físico punto a punto entre dos nodos. El término enlace lógico incluye asimismo los múltiples canales lógicos X.25 que comparten el uso del enlace de acceso desde un DTE a una red X.25.

enlace virtual (virtual link). En OSPF (abrir primero la vía más corta), interfaz punto a punto que conecta direccionadores limítrofes separados por un área de tránsito no de red troncal. Debido a que los direccionadores del área forman parte de la red troncal de OSPF, el enlace virtual conecta la red troncal. Los enlaces virtuales garantizan que la red troncal de OSPF no se vuelva discontinua.

equipo de conmutación de datos (data switching exchange) (DSE). Equipo que se instala en una sola ubicación para proporcionar funciones de conmutación como, por ejemplo, la conmutación de circuitos, la conmutación de mensajes y la conmutación de paquetes. (I)

equipo de terminación de circuito de datos (data circuit-terminating equipment) (DCE). En una estación de datos, equipo que proporciona la conversión y la codificación de señal entre el equipo terminal de datos (DTE) y la línea. (I)

Notas:

1. El DCE puede ser un equipo aparte o una parte integrante del DTE o del equipo intermedio.
2. Un DCE puede realizar otras funciones que suelen realizarse en el extremo red de la línea.

Equipo Negociador de Ingeniería de Internet (Internet Engineering Task Force) (IETF). Equipo negociador de Internet Architecture Board (IAB), responsable de resolver las necesidades de ingeniería a corto plazo de Internet.

equipo terminal de datos (data terminal equipment) (DTE). La parte de una estación de datos que hace de fuente de datos, sumidero de datos, o ambas cosas. (I) (A)

esfera de control (sphere of control) (SOC). Conjunto de dominios de punto de control servidos por un solo punto focal de servicios de gestión.

estación (station). Punto de entrada o de salida de un sistema que utiliza servicios de telecomunicaciones; por ejemplo, uno o varios sistemas, PC, terminales, dispositivos y programas asociados de una ubicación determinada que puede enviar o recibir datos a través de una línea de telecomunicaciones.

estación de configuración de conmutador Nways (Nways Switch configuration station). Estación OS/2 dedicada que ejecuta una versión autónoma de la

herramienta NCT (Nways Switch Configuration Tool). Se utiliza para generar una base de datos de configuración de red y debe instalarse como consola remota.

estación de enlace (link station). (1) Componentes de hardware y software que hay en un nodo y que representan una conexión con un nodo adyacente a través de un enlace específico. Por ejemplo, el nodo A, si es el extremo primario de una línea multipunto que se conecta a tres nodos adyacentes, tendría tres estaciones de enlace que representarían las conexiones con los nodos adyacentes. (2) Véase también *estación de enlace adyacente (ALS)*.

estación de gestión (management station). En las comunicaciones Internet, sistema responsable de gestionar la totalidad o parte de una red. La estación de gestión se comunica con los agentes de gestión de red que residen en un nodo gestionado, utilizando un protocolo de gestión de red, como puede ser el protocolo simple de gestión de red (SNMP).

estación de gestión de red (network management station). En el protocolo simple de gestión de red (SNMP), estación que ejecuta los programas de aplicación de gestión que supervisan y controlan los elementos de la red.

estación de soporte de red (network support station). Procesador utilizado para operar lógicamente y dar servicio al conmutador Nways. Lo utilizan el administrador o el personal de servicio del conmutador Nways.

estado de enlace (link-state). En los protocolos de direccionamiento, información anunciada acerca de las interfaces utilizables y de los vecinos accesibles de un direccionador o de una red. La base de datos topológica del protocolo se forma a partir de los anuncios recogidos sobre el estado de enlace.

estructura de información de gestión (Structure of Management Information) (SMI). (1) En el protocolo simple de gestión de red (SNMP), reglas utilizadas para definir los objetos a los que se puede acceder por medio de un protocolo de gestión de red. (2) En OSI, conjunto de estándares relacionados con la información de gestión. El conjunto incluye el *Modelo de información de gestión* y las *Directrices para la definición de objetos gestionados*

Ethernet. Red de área local de banda base de 10 Mbps que permite a múltiples estaciones acceder a voluntad al medio de transmisión sin coordinación previa, evita la contienda utilizando la detección de portadora y la deferencia, y resuelve la contienda mediante la detección de colisión y la retransmisión diferida. Ethernet utiliza el acceso múltiple con detección de portadora y detección de colisión (CSMA/CD).

excepción (exception). Condición anómala como, por ejemplo, encontrar un error de E/S en el proceso de un conjunto de datos o de un archivo.

extensión de ruta (route extension) (REX). En SNA, componentes de red de control de vía, incluido un enlace periférico, que constituyen la parte de una vía entre un nodo de subárea y una unidad de red direccionable (NAU) de un nodo periférico adyacente. Véase también *ruta explícita (ER)*, *vía* y *ruta virtual (VR)*.

F

fax. Copia impresa que se recibe desde una máquina de fax. Sinónimo con ***telecopia.***

fluctuación (jitter). (1) Variaciones no acumulativas a corto plazo de los instantes significativos de una señal digital en relación a la posición ideal que tendría en el tiempo. (2) Variaciones no deseables de una señal digital transmitida. (3) Variaciones del retardo de red.

fragmentación (fragmentation). (1) Proceso de dividir un datagrama en partes más pequeñas, o fragmentos, para ajustarse a las posibilidades del medio físico a través del que se va a transmitir. (2) Véase también *segmentación*.

fragmento (fragment). Véase *fragmentación*.

frame relay. (1) Interfaz estándar que describe el límite entre el equipo de un usuario y una red de paquetes rápidos. En los sistemas frame-relay, las tramas defectuosas se descartan; la recuperación se realiza entre extremos, en vez de entre saltos. (2) Técnica derivada del estándar del canal D de la red digital de servicios integrados (RDSI). Presupone que las conexiones son fiables y prescinde de la actividad general que supone la detección de errores y el control dentro de la red.

G

gestión de red (network management). Proceso de planificar, organizar y controlar un proceso de datos o un sistema de información orientado a la comunicación.

gestor de red (network manager). Programa o grupo de programas que se utiliza para supervisar, gestionar y diagnosticar los problemas de una red.

Grabación de cambios en unos sin retorno a cero (Non-Return-to-Zero Changes-on-Ones Recording) (NRZ-1). Método de grabación en el que los unos vienen representados por un cambio en la condición de magnetización y los ceros vienen representados por la ausencia de cambio. Sólo se graban explícitamente las señales de los unos. (Anteriormente se llamaba grabación ***inversión sin retorno a cero***, NRZI.)

grupo de transmisión (transmission group) (TG). (1) Conexión entre nodos adyacentes que se identifica mediante un número de grupo de transmisión. (2) En una red de subárea, enlace individual o grupo de enlaces entre nodos adyacentes. Cuando un grupo de transmisión consta de un grupo de enlaces, éstos se ven como un único enlace lógico y el grupo de transmisión se llama *grupo de transmisión multienlace (MLTG)*.

Llamamos *grupo de transmisión multienlace de medios mixtos (MMMLTG)* a un grupo que contiene enlaces de distintos tipos de medio (por ejemplo, enlaces de red en anillo, SDLC conmutado, SDLC no conmutado y frame-relay). (3) En una red APPN, enlace individual entre nodos adyacentes. (4) Véase también *grupos de transmisión en paralelo.*

grupos de transmisión en paralelo (parallel transmission groups). Múltiples grupos de transmisión entre nodos adyacentes, teniendo cada grupo un número diferenciado de grupo de transmisión.

H

Hello. Protocolo que utilizan un grupo de direccionadores de confianza que cooperan y que les permite descubrir las rutas de retardo mínimo.

heurístico (heuristic). Perteneciente a los métodos exploratorios de resolución de problemas en los que las soluciones se descubren mediante la evaluación del progreso realizado hacia el resultado final.

histéresis (hysteresis). Antes de que la condición de alerta desaparezca, debe haber un cambio en la temperatura que la haga pasar el umbral de establecimiento de alerta.

horizonte dividido (split horizon). Técnica para minimizar el tiempo en el que se llega a la convergencia de la red. Un direccionador registra la interfaz a través de la que ha recibido una ruta determinada y no propaga la información sobre la ruta de vuelta a través de la misma interfaz.

I

identificación de intercambio (exchange identification) (XID). Tipo específico de unidad de enlace básico que se utiliza para comunicar las características de nodo y enlace entre nodos adyacentes. Los XID se intercambian entre las estaciones de enlace antes y durante la activación del enlace para establecer y negociar las características de nodo y enlace, y después de la activación del enlace para comunicar los cambios que se hayan realizado en estas características.

identificador de conexión de enlace de datos (data link connection identifier) (DLCI). Identificador numérico de un subpuerto de frame-relay o de un segmento PVC de una red frame-relay. Cada uno de los subpuertos de un puerto frame-relay individual tiene un DLCI exclusivo. En la tabla siguiente, según el estándar T1.618 de ANSI (American National Standards Institute) y el estándar Q.922 del Comité Consultivo Internacional de Telegrafía y Telefonía (ITU-T/CCITT), se indican las funciones asociadas a determinados valores de DLCI:

Valores de DLCI	Función
0	señalización de canal de entrada
1–15	reservados
16–991	asignados al uso de procedimientos de conexión frame-relay
992–1007	gestión de la capa 2 del servicio de soporte a frame-relay
1008–1022	reservados
1023	gestión de capas de canal de entrada

identificador de puente (bridge identifier). Campo de 8 bytes, utilizado en un protocolo de árbol de extensión, que consta de la dirección MAC del puerto cuyo identificador sea el más pequeño y de un valor definido por el usuario.

identificador de red (network identifier). (1) En TCP/IP, parte de la dirección IP que define una red. La longitud del ID de red depende de qué tipo es 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 modo exclusivo una subred específica.

inhabilitado (disabled). (1) Relativo al estado de una unidad de proceso que impide la aparición de determinados tipos de interrupciones. (2) Relativo al estado en el que una unidad de control de transmisión o una unidad de respuesta de sonido no puede aceptar las llamadas entrantes de una línea.

inhabilitar (disable). Hacer que no funcione.

intercambio de paquetes interredes (Internetwork Packet Exchange) (IPX). (1) Protocolo de red utilizado para conectar servidores de Novell, o cualquier estación de trabajo o direccionador que implemente IPX, con otras estaciones de trabajo. Aunque sea parecido a IP (protocolo Internet), IPX utiliza otros formatos de paquete y una terminología diferente. (2) Véase también *Xerox Network Systems (XNS).*

interconexión de sistemas abiertos (Open Systems Interconnection) (OSI). (1) Interconexión de los sistemas abiertos de acuerdo con los estándares de ISO (Organización Internacional para la Normalización) para el intercambio de información. (T) (A) (2) Uso de procedimientos estandarizados para habilitar la interconexión de sistemas de proceso de datos.

Nota: La arquitectura OSI establece una infraestructura que permite coordinar el desarrollo de estándares actuales y futuros para la interconexión de sistemas informáticos. Las funciones de red se dividen en siete capas. Cada una de ellas representa un grupo de funciones relacionadas de proceso de datos y de comunicaciones que pueden llevarse a cabo de forma estándar para dar soporte a las distintas aplicaciones.

interfaz (interface). (1) Frontera compartida entre dos unidades funcionales y definida mediante

características funcionales y características de señal, entre otras, según corresponda. El concepto incluye la especificación de la conexión de dos dispositivos que tengan funciones diferentes. (T) (2) Hardware, software, o ambas cosas, que enlaza sistemas, programas o dispositivos.

interfaz de gestión local (local management interface) (LMI). Véase *protocolo de interfaz de gestión local (LMI)*.

interfaz de unidad de conexión (attachment unit interface) (AUI). En una red de área local, interfaz entre la unidad de conexión de medio y el equipo terminal de datos dentro de una estación de datos. (I) (A)

Internet. Conjunto de redes administrados por IAB (Internet Architecture Board) y que consta de grandes redes troncales nacionales y de muchas redes regionales y universitarias de todo el mundo. Internet utiliza la serie de protocolos de Internet.

Internet Architecture Board (IAB). Cuerpo técnico que inspecciona el desarrollo de la serie de protocolos de Internet conocidos como TCP/IP.

interoperatividad (interoperability). Posibilidad de comunicar, ejecutar programas o transferir datos entre diversas unidades funcionales de tal manera que el usuario apenas necesite conocer las características exclusivas de dichas unidades. (T)

interredes. Conjunto de redes interconectadas por un grupo de direccionadores que permiten a las redes funcionar como si fuesen una sola red de gran tamaño. Véase también *Internet*.

IPPN. Interfaz que otros protocolos pueden usar para transportar datos a través de IP.

IPXWAN. Protocolo de Novell que se utiliza para intercambiar información entre direccionadores antes de intercambiar la información IPX (intercambio de paquetes interredes) y el tráfico a través de las redes de área amplia (WAN).

L

LAN Network Manager (LNM). Programa bajo licencia de IBM que permite a un usuario gestionar y supervisar los recursos de LAN desde una estación de trabajo central.

línea tronco (trunk line). Línea de alta velocidad que conecta dos conmutadores Nways. Puede tratarse, por ejemplo, de un cable coaxial, un cable de fibra o una onda de radio, y pueden alquilarse en las compañías de telecomunicaciones.

local. (1) Dícese del dispositivo al que se accede directamente, sin utilizar una línea de telecomunicaciones. (2) Contrástese con *remoto*. (3) Sinónimo de *conectado por canal*.

M

mandato ping (ping command). Mandato que envía un paquete de petición de eco ICMP (protocolo de mensaje de control de Internet) a una pasarela, a un direccionador o a un sistema principal con la esperanza de recibir una respuesta.

máscara - enmascarar (mask). (1) Patrón de caracteres utilizado para controlar la retención o la eliminación de partes de otro patrón de caracteres. (I) (A) (2) Utilizar un patrón de caracteres para controlar la retención o la eliminación de partes de otro patrón de caracteres. (I) (A)

máscara de dirección (address mask). Para subredes de internet, máscara de 32 bits utilizada para identificar los bits de la dirección de subred en la parte de sistema principal de una dirección IP. Sinónimo con *máscara de subred*.

máscara de subred (subnet mask). Sinónimo de *máscara de dirección*.

máscara de subred (subnetwork mask). Sinónimo de *máscara de dirección*.

memoria de almacenamiento dinámico (heap memory). Cantidad de RAM utilizada para asignar dinámicamente estructuras de datos.

memoria de sólo lectura (read-only memory) (ROM). Memoria en la que el usuario no puede modificar los datos almacenados, a no ser en condiciones especiales.

memoria flash (flash memory). Dispositivo de almacenamiento de datos programable, borrable y que no requiere alimentación continua. La ventaja principal que tiene la memoria flash sobre los demás dispositivos de almacenamiento de datos programables y borrables es que se puede reprogramar sin desmontarla de la placa de circuitos.

mensaje hello (hello message). (1) Mensaje que se envía periódicamente para establecer y comprobar la accesibilidad entre direccionadores o entre direccionadores y sistemas principales. (2) En la serie de protocolos de Internet, mensaje definido por el protocolo Hello como protocolo IGP (protocolo de pasarela interior).

métrica (metric). En las comunicaciones Internet, valor, asociado a una ruta, que se utiliza para discriminar entre múltiples puntos de salida o de entrada en un mismo sistema autónomo. La ruta preferida es la que tiene la métrica más baja.

MIB. (1) Módulo MIB. (2) Base de información de gestión.

MIB estándar (standard MIB). En el protocolo simple de gestión de red (SNMP), módulo MIB que se encuentra en la rama de gestión de la estructura de información de gestión (SMI), considerado como estándar por el Equipo Negociador de Ingeniería de Internet (IETF).

MILNET. La red militar que en un principio formaba parte de ARPANET. Se separó de ARPANET en 1984. MILNET proporciona un servicio de red fiable a las instalaciones militares.

modelo de referencia de interconexión de sistemas abiertos (OSI reference model). Modelo que describe los principios generales de la interconexión de sistemas abiertos, así como la finalidad y la disposición jerárquica de las siete capas de esta arquitectura. (T)

módem (modulador/demodulador) (modem). (1) Unidad funcional que modula y demodula señales. Una de las funciones de un módem es permitir que los datos digitales se transmitan a través de recursos de transmisión analógicos. (T) (A) (2) Dispositivo que convierte los datos digitales de un sistema informático en una señal analógica que puede transmitirse en una línea de telecomunicaciones, y convierte la señal analógica recibida en datos para el sistema informático.

modulación por impulsos codificados (pulse code modulation) (PCM). Estándar adoptado para la digitalización de una señal de voz analógica. En PCM, la voz se muestrea con una frecuencia de ocho kHz y cada muestra se codifica en una trama de 8 bits.

módulo (module). En la conmutación Nways, unidad de hardware funcional empaquetada que contiene tarjetas lógicas, conectores e indicadores luminosos. Los módulos se utilizan para empaquetar adaptadores, acopladores de interfaz de línea, extensiones de servidor de voz y otros componentes. Todos los módulos son ***conectables dinámicos*** en las subestanterías lógicas.

módulo (modulo). (1) Relativo a un módulo; por ejemplo, 9 es equivalente a 4 módulo 5. (2) Véase también *módulo (modulus)*.

módulo (modulus). En una relación, número (que puede ser un entero positivo) que es divisor exacto (no deja resto) de la diferencia entre los dos números relacionados; por ejemplo, el módulo de 9 y 4 es 5 (9 - 4 = 5; 4 - 9 = -5; y 5 es divisor exacto tanto de 5 como de -5, pues no deja resto).

multidifusión (multicast). (1) Transmisión de unos mismos datos a un grupo seleccionado de destinos. (T) (2) Forma especial de difusión general en la que las copias de un paquete se entregan únicamente a un subconjunto de todos los destinos posibles.

multiplexado por división de tiempo (time division multiplexing) (TDM). Véase ***canalización***.

N

NetBIOS. Network Basic Input/Output System (sistema básico de entrada/salida de red). Interfaz estándar para redes, sistemas IBM Personal Computer (PC) y sistemas 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 los protocolos de control de enlace de datos (DLC) de las LAN.

nivel de enlace (link level). (1) Parte de la recomendación X.25 que define el protocolo de enlace utilizado para hacer que los datos entren y salgan de la red a través del enlace dúplex que conecta la máquina del suscriptor con el nodo de red. LAP y LAPB son los protocolos de acceso de enlace recomendados por CCITT. (2) Véase *nivel de enlace de datos*.

nivel de enlace de datos (data link level). (1) En la estructura jerárquica de una estación de datos, nivel conceptual de la lógica de control o 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 como las de insertar bits de transmisión y suprimir bits de recepción; interpretar campos de dirección y de control; generar, transmitir e interpretar mandatos y respuestas; así como calcular e interpretar secuencias de comprobación de trama. Véase también *nivel de paquete* y *nivel físico*. (2) En las comunicaciones X.25, sinónimo de *nivel de trama*.

nivel de trama (frame level). Sinónimo con *nivel de enlace de datos*. Véase *nivel de enlace*.

nodo (node). (1) En una red, punto al que una o varias unidades funcionales conectan canales o circuitos de datos. (I) (2) Cualquier dispositivo, conectado a una red, que transmite y recibe datos.

nodo (node) de comunicaciones avanzadas de igual a igual (APPN). Nodo de red APPN o nodo final APPN.

nodo de esfera de control (sphere of control (SOC) node). Nodo que está directamente en la esfera de control de un punto focal. Un nodo SOC tiene elementos de habilitación de servicios de gestión intercambiados con el punto focal que le corresponde. Un nodo final APPN puede ser un nodo SOC si da soporte a la función de intercambiar elementos de habilitación de los servicios de gestión.

nodo de red (network node) (NN). Véase *nodo de red de comunicaciones avanzadas de igual a igual (APPN)*.

nodo de red (network node) de comunicaciones avanzadas de igual a igual (APPN). Nodo que ofrece una amplia gama de servicios de usuario final y que puede proporcionar los servicios siguientes:

- Servicios de directorio distribuido, incluido el registro de los recursos de dominio en un servidor de directorios central
- Intercambios de base de datos de topología con otros nodos de red APPN, habilitando los nodos de red en toda la red para seleccionar las rutas óptimas de sesiones LU-LU en función de las clases de servicio solicitadas
- Servicios de sesión para las LU locales y los nodos finales clientes
- Servicios de direccionamiento intermedio dentro de una red APPN

nodo de red APPN (APPN network node). Véase *nodo de red de comunicaciones avanzadas de igual a igual (APPN)*.

nodo de red de entrada limitada (low-entry networking (LEN) node). Nodo que proporciona una gama de servicios de usuario final, se conecta directamente a otros nodos mediante protocolos de igual a igual, y deriva implícitamente servicios de red de un nodo de red APPN adyacente, es decir, sin el uso directo de sesiones CP-CP.

nodo destino (destination node). Nodo al que se envía una petición o datos.

nodo final (end node) (EN). (1) Véase *nodo final de comunicaciones avanzadas de igual a igual (APPN)* y *nodo final de redes de entrada limitada (LEN)*. (2) En comunicaciones, nodo que con frecuencia se conecta a un solo enlace de datos y no puede realizar funciones de direccionamiento intermedio.

nodo final (end node) de comunicaciones avanzadas de igual a igual (APPN). Nodo que proporciona una amplia gama de servicios de usuario final y da soporte a sesiones entre el punto de control (CP) local que le corresponde y el punto de control de un nodo de red adyacente. Utiliza estas sesiones para registrar dinámicamente sus recursos en el CP adyacente (el servidor de nodo de red que le corresponde), enviar y recibir peticiones de búsqueda en directorio y obtener servicios de gestión. Un nodo final APPN puede asimismo conectarse a una red de subárea como nodo periférico o conectarse a otros nodos finales.

nodo final de red de entrada limitada (low-entry networking (LEN) end node). Nodo LEN que recibe servicios de red de un nodo de red APPN adyacente.

nodo intermedio (intermediate node). Nodo que está en el extremo de más de una rama. (T)

nodos adyacentes (adjacent nodes). Dos nodos conectados entre sí mediante al menos una vía que no se conecta a ningún otro nodo. (T)

nombre de comunidad (community name). En el protocolo simple de gestión de red (SNMP), serie de octetos que identifican una comunidad.

nombre de dominio (domain name). En la serie de protocolos de Internet, nombre de un sistema principal. El nombre de dominio consta de una secuencia de subnombres separados por un carácter delimitador. Por ejemplo, si el nombre de dominio totalmente calificado (FQDN) de un sistema principal es `ralvm7.vnet.ibm.com`, cada uno de los nombres siguientes es un nombre de dominio:

- `ralvm7.vnet.ibm.com`
- `vnet.ibm.com`
- `ibm.com`

notación de sintaxis abstracta (abstract syntax notation) 1 (ASN.1). Método de OSI (interconexión de sistemas abiertos) para la sintaxis abstracta, que se especifica en los estándares siguientes:

- ITU-T Recomendación X.208 (1988) | ISO/IEC 8824: 1990
- ITU-T Recomendación X.680 (1994) | ISO/IEC 8824-1: 1994

Véase también *reglas básicas de codificación (BER)*.

notación decimal con puntos (dotted decimal notation). Representación sintáctica de un entero de 32 bits que consta de cuatro números de 8 bits escritos en base 10 y separados entre sí mediante puntos. Se utiliza para representar direcciones IP.

número de puerto (port number). En las comunicaciones Internet, identificación de una entidad de aplicación en el servicio de transporte.

número de secuencia (sequence number). En comunicaciones, número asignado a una determinada trama o paquete para controlar el flujo de transmisión y la recepción de los datos.

número de sistema autónomo (autonomous system number). En TCP/IP, número asignado a un sistema autónomo por la misma autoridad central que asigna también las direcciones IP. Mediante este número, los algoritmos de direccionamiento automatizado pueden distinguir entre los sistemas autónomos.

O

objeto MIB (MIB object). Sinónimo de *variable MIB*.

operación en modalidad de paquetes (packet mode operation). Sinónimo de *conmutación de paquetes*.

Organización Internacional para la Normalización (International Organization for Standardization) (ISO). Organización de corporaciones de estándares nacionales de diversos países establecida para promocionar el desarrollo de estándares con el fin de facilitar el intercambio internacional de bienes y servicios, y de desarrollar la cooperación en el campo intelectual, científico, tecnológico y económico.

origen (origin). Unidad lógica (LU) externa o programa de aplicación que produce un mensaje u otros datos. Véase también *destino*.

P

paquete (packet). En la comunicación de datos, secuencia de dígitos binarios que incluyen datos y señales de control, y se transmiten y conmutan como un todo compuesto. Los datos, las señales de control y, posiblemente, la información de control de errores se organizan con un formato específico. (I)

paquete de datos (data packet). En las comunicaciones X.25, paquete que se utiliza para la transmisión de datos de usuario en un circuito virtual, en la interfaz DTE/DCE.

paquete de petición de llamada (call request packet). (1) Paquete de supervisión de llamada transmitido por

un equipo terminal de datos (DTE) para pedir el establecimiento de conexión de una llamada en toda la red. (2) En las comunicaciones X.25, paquete de supervisión de llamada transmitido por un DTE para pedir el establecimiento de una llamada en toda la red.

paquete de petición de restablecimiento (reset request packet). En las 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. La razón de la petición puede especificarse asimismo en el paquete.

paquete de recepción no preparada (receive not ready (RNR) packet). Véase *paquete RNR*.

paquete explorador (explorer packet). En las LAN, paquete generado por un sistema principal origen y que atraviesa toda la parte de direccionamiento en origen de una LAN reuniendo información sobre las posibles vías disponibles para el sistema principal.

paquete RNR (RNR packet). Paquete utilizado por un equipo terminal de datos (DTE) o por un equipo de terminación de circuito de datos (DCE) para indicar la imposibilidad temporal de aceptar paquetes adicionales de una llamada virtual o de un circuito virtual permanente.

parámetro de configuración (configuration parameter). Variable de una definición de configuración, cuyos valores pueden caracterizar la relación de un producto con los demás productos de una misma red o que pueden definir las características del propio producto.

pasarela (gateway). (1) Unidad funcional que interconecta dos redes de sistemas que tienen distintas arquitecturas de red. Las pasarelas conectan redes o sistemas de distintas arquitecturas. Los puentes interconectan redes o sistemas cuya arquitectura sea igual o semejante. (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 a un sistema principal que utilizan distintos protocolos de enlace lógico. (3) En TCP/IP, sinónimo de *direccionador*.

pasarela exterior (exterior gateway). En las comunicaciones Internet, pasarela situada en un sistema autónomo que comunica con otro sistema autónomo. Contrástese con *pasarela interior*.

pasarela interior (interior gateway). En las comunicaciones Internet, pasarela que solamente establece comunicación con su propio sistema autónomo. Contrástese con *pasarela exterior*.

petición de comentarios (Request for Comments) (RFC). En las comunicaciones Internet, serie de documentos que describe una parte de la serie de protocolos de Internet y los experimentos relacionados. Todos los estándares de Internet se han documentado como RFC.

peticionario de LU dependiente (dependent LU requester) (DLUR). Nodo final APPN o nodo de red APPN que es propietario de unidades lógicas (LU) dependientes, pero solicita que un servidor LU dependiente proporcione los servicios SSCP a dichas LU dependientes.

por omisión (default). Dícese del atributo, condición, valor u opción que se toma cuando no se ha definido ninguno explícitamente. (I)

portadora (carrier). Onda o tren de impulsos eléctricos o magnéticos que una señal puede activar y que lleva información que se ha de transmitir por un sistema de comunicaciones. (T)

procesador frontend (front-end processor). Procesador, como el 3745 o el 3174 de IBM, que libra a un sistema central de las tareas de control de comunicaciones.

proceso en tiempo real (real-time processing). Manipulación por parte de un proceso de los datos que se requieren o se generan, mientras dicho proceso está operativo. Con frecuencia, los resultados se utilizan para influenciar el propio proceso (y tal vez también los procesos relacionados) mientras se está produciendo.

protocolo (protocol). (1) Conjunto de reglas semánticas y sintácticas que determinan el comportamiento de las unidades funcionales para lograr comunicarse. (I) (2) En la arquitectura OSI (interconexión de sistemas abiertos), conjunto de reglas semánticas y sintácticas que determinan el comportamiento de las entidades de una misma capa al realizar funciones de comunicación. (T) (3) En SNA, significados y reglas de ordenación de las peticiones y respuestas utilizadas 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 de corchete* y *protocolo de enlace*.

protocolo de acceso a subred (Subnetwork Access Protocol) (SNAP). En las LAN, discriminador de protocolo de 5 bytes que identifica la familia de protocolos estándar no IEEE al que pertenece el paquete. El valor SNAP se utiliza para distinguir entre los protocolos que utilizan `$AA` como valor de punto de acceso a servicio (SAP).

protocolo de acceso de enlace equilibrado (link access protocol balanced) (LAPB). Protocolo utilizado para acceder a una red X.25 a nivel de enlace. LAPB es un protocolo dúplex, asíncrono y simétrico que se utiliza en la comunicación punto a punto.

protocolo de actualización de direccionamiento (RouTing update Protocol) (RTP). Protocolo de VINES (VIrtual NEtworking System) que mantiene la base de datos de direccionamiento y permite el intercambio de información de direccionamiento entre nodos VINES. Véase también *protocolo de control de Internet (ICP)*.

protocolo de anuncio de servicio (Service Advertising Protocol) (SAP). En IPX (intercambio de paquetes

interredes), protocolo que proporciona los mecanismos siguientes:

- Un mecanismo que permite a los servidores IPX de un conjunto de redes anunciar sus servicios por nombre y por tipo. Los servidores que utilizan este protocolo tienen registrados su nombre, tipo de servicio y dirección en todos los servidores de archivos que ejecutan NetWare.
- Un mecanismo que permite a una estación de trabajo difundir una consulta para descubrir las identidades de todos los servidores de todos los tipos, de todos los servidores de un tipo específico, o del servidor más cercano de un tipo específico.
- Un mecanismo que permite a una estación de trabajo consultar cualquier servidor de archivos que ejecute NetWare para descubrir los nombres y las direcciones de todos los servidores de un tipo específico.

protocolo de control de acceso al medio (MAC protocol). En una red de área local, protocolo que rige el acceso al medio de transmisión, tomando en consideración los aspectos topológicos de la red, para habilitar el intercambio de datos entre las estaciones de datos. (T)

protocolo de control de enlace lógico (logical link control (LLC) protocol). En una red de área local, protocolo que rige el intercambio de tramas de transmisión entre las estaciones de datos con independencia de cómo se comparte el medio de transmisión. (T) El protocolo LLC ha sido desarrollado por el comité IEEE 802 y es común a todos los estándares de LAN.

protocolo de control de Internet (Internet Control Protocol) (ICP). Protocolo de VINES (VIrtual NEtworking System) que proporciona notificaciones de excepciones, notificaciones de métrica y soporte para PING. Véase también *protocolo de actualización de direccionamiento (RTP)*.

protocolo de control de transmisión (Transmission Control Protocol) (TCP). Protocolo de comunicaciones utilizado en Internet y en cualquier red que se ajuste a los estándares del Departamento de Defensa de los Estados Unidos para el protocolo interredes. TCP proporciona un protocolo sistema a sistema fiable entre los sistemas principales que hay en las redes de comunicaciones de paquetes conmutados y en los sistemas interconectados de dichas redes. Como protocolo subyacente, utiliza el protocolo Internet (IP).

Protocolo de control de transmisión/protocolo Internet (Transmission Control Protocol/Internet Protocol) (TCP/IP). Conjunto de protocolos de comunicaciones que dan soporte a las funciones de conectividad de igual a igual para las redes tanto de área local como de área amplia.

protocolo de datagrama de usuario (User Datagram Protocol) (UDP). En la serie de protocolos de Internet, protocolo que proporciona un servicio de datagrama no fiable y sin conexiones. Permite que un programa de aplicación de una máquina o de un proceso envíe un datagrama a un programa de aplicación de otra máquina o proceso. UDP utiliza el protocolo Internet (IP) para entregar datagramas.

protocolo de direccionamiento (routing protocol). Técnica utilizada por un direccionador para localizar los demás direccionadores y para mantenerse informado acerca de cuál es el mejor camino que lleva a las redes accesibles.

protocolo de ejecución remota (Remote Execution Protocol) (REXEC). Protocolo que permite la ejecución de un mandato o de un programa en cualquier sistema principal de la red. El sistema principal recibe los resultados de la ejecución del mandato.

protocolo de enlace de nombre (Name Binding Protocol) (NBP). En las redes AppleTalk, protocolo que proporciona la función de conversión del nombre (serie de caracteres) de la entidad (recurso) AppleTalk a la dirección IP (número de 16 bits) de AppleTalk en la capa de transporte.

protocolo de entrega de datagramas (Datagram Delivery Protocol) (DDP). En las redes AppleTalk, protocolo que proporciona conectividad de red por medio de un servicio de entrega sin conexiones de socket a socket en la capa interredes.

protocolo de información de direccionamiento (Routing Information Protocol) (RIP). En la serie de protocolos de Internet, protocolo de pasarela interior utilizado para intercambiar información de direccionamiento intradominio y para determinar cuáles son las rutas óptimas entre los sistemas principales de Internet. RIP determina las rutas óptimas basándose en la métrica de ruta, no en la velocidad de transmisión de los enlaces.

protocolo de información territorial (Zone Information Protocol) (ZIP). En las redes AppleTalk, protocolo que proporciona servicio de gestión territorial manteniendo una correlación entre los nombres de zona y los números de red a lo largo del conjunto de redes en la capa de sesión.

protocolo de interfaz de gestión local (local management interface (LMI) protocol). En NCP, conjunto de procedimientos y mensajes de gestión de red frame-relay utilizados por los nodos frame-relay adyacentes para intercambiar información de estado de línea a través de DLCI X'00'. NCP da soporte tanto a la versión de American National Standards Institute (ANSI) como a la versión del Comité Consultivo Internacional de Telegrafía y Telefonía (ITU-T/CCITT) del protocolo LMI. Estos estándares hacen referencia al protocolo LMI como *pruebas de verificación de integridad de enlace (LIVT)*.

protocolo de mantenimiento de la tabla de direccionamiento (Routing Table Maintenance Protocol) (RTMP). En las redes AppleTalk, protocolo que proporciona la generación y el mantenimiento de información de direccionamiento en la capa de transporte por medio de la tabla de direccionamiento

de AppleTalk. Esta tabla dirige la transmisión de paquetes a través del conjunto de redes desde el socket origen hasta el socket destino.

protocolo de mensajes de control de Internet (Internet Control Message Protocol) (ICMP). Protocolo utilizado para manejar mensajes de error y de control en la capa IP (protocolo Internet). Los informes de problemas y de destinos de datagrama incorrectos se devuelven a la fuente de datagramas original. ICMP forma parte del protocolo Internet (IP).

protocolo de pasarela exterior (Exterior Gateway Protocol) (EGP). En la serie de protocolos de Internet, protocolo que se utiliza entre dominios y sistemas autónomos y que permite anunciar e intercambiar información de accesibilidad de red. Las direcciones de red IP de un sistema autónomo se anuncian a otro sistema autónomo por medio de direccionadores participantes de EGP. Ejemplo de un EGP es el protocolo de pasarela limítrofe (BGP). Contrástese con el protocolo de pasarela interior (IGP).

protocolo de pasarela interior (Interior Gateway Protocol) (IGP). En la serie de protocolos de Internet, protocolo utilizado para propagar accesibilidad de red e información de direccionamiento dentro de un sistema autónomo. Ejemplos de IGP son el protocolo RIP (protocolo de información de direccionamiento) y OSPF (abrir primero la vía más corta).

protocolo de pasarela limítrofe (Border Gateway Protocol) (BGP). Protocolo de direccionamiento IP (Internet Protocol) que se utiliza entre dominios y sistemas autónomos.

protocolo de resolución de direcciones (Address Resolution Protocol) (ARP). (1) En la serie de protocolos de Internet, protocolo que correlaciona dinámicamente una dirección IP con una dirección utilizada por una red de área local o metropolitana de soporte, como Ethernet o una red en anillo. (2) Véase también *protocolo de resolución de direcciones invertidas (RARP).*

protocolo de resolución de direcciones AppleTalk (AppleTalk Address Resolution Protocol) (AARP). En las redes AppleTalk, protocolo que (a) convierte las direcciones de nodo AppleTalk en direcciones de hardware y (b) concilia las discrepancias de direccionamiento en las redes que dan soporte a más de un conjunto de protocolos.

protocolo de resolución inversa de direcciones (Inverse Address Resolution Protocol) (InARP). En la serie de protocolos de Internet, protocolo utilizado para localizar una dirección de protocolo mediante la dirección de hardware conocida. En un contexto de frame-relay, el identificador de conexión de enlace de datos (DLCI) es sinónimo con la dirección de hardware conocida.

protocolo de transacciones AppleTalk (AppleTalk Transaction Protocol) (ATP). En las redes AppleTalk, protocolo que proporciona funciones de petición y respuesta de cliente/servidor para los sistemas principales que acceden al protocolo de información territorial (ZIP) para obtener información territorial.

protocolo de transferencia de archivos (File Transfer Protocol) (FTP). En la serie de protocolos de Internet, protocolo de la capa de aplicación que utiliza los servicios TCP y Telnet para transferir archivos de datos generales entre máquinas o sistemas principales.

protocolo Internet (Internet Protocol) (IP). Protocolo sin conexiones que direcciona los datos a través de una red o de redes interconectadas. IP hace de intermediario entre las capas de protocolo más altas y la red física. Sin embargo, este protocolo no proporciona recuperación de errores ni control de flujo, ni tampoco queda garantizada la fiabilidad de la red física.

protocolo Internet de línea serie (Serial Line Internet Protocol) (SLIP). Protocolo utilizado a través de una conexión punto a punto entre dos sistemas principales IP a lo largo de una línea serie como, por ejemplo, un cable serie o una conexión RS232 con un módem, por línea telefónica.

protocolo punto a punto (Point-to-Point Protocol) (PPP). Protocolo que proporciona un método para encapsular y transmitir paquetes a través de enlaces serie punto a punto.

protocolo simple de gestión de red (Simple Network Management Protocol) (SNMP). En la serie de protocolos de Internet, protocolo de gestión de red que se emplea para supervisar los direccionadores y las redes conectadas. SNMP es un protocolo de la capa de la aplicación. La información sobre los dispositivos gestionados se define y almacena en la MIB (base de información de gestión) de la aplicación.

prueba de bucle de retorno (loopback test). Prueba en la que las señales de un tester se envían a un módem o a otro elemento de red y retornan al tester para obtener mediciones que determinen o verifiquen la calidad de la vía de comunicaciones.

puente (bridge). Unidad funcional que interconecta varias LAN (local o remotamente) que utilizan un mismo protocolo de control de enlace lógico, aunque pueden utilizar distintos protocolos de control de acceso al medio. Un puente reenvía una trama a otro puente basándose en la dirección MAC (control de acceso al medio).

puente de ruta (route bridge). Función de un programa de puente IBM que permite a dos sistemas informáticos puente utilizar un enlace de telecomunicaciones para conectar dos LAN. Cada sistema puente se conecta directamente a una de las LAN, y el enlace de telecomunicaciones conecta los dos sistemas puente.

puente raíz (root bridge). Puente que es la raíz del árbol de extensión formado entre otros puentes activos de la red de puenteo. El puente raíz origina y transmite las unidades de datos de protocolo de puente (BPDU) a los demás puentes activos para mantener la topología

del árbol de extensión. Es el puente de prioridad más alta de la red.

puenteo (bridging). En las LAN, reenvío de una trama desde un segmento a otro de la LAN. El destino se especifica mediante la dirección de subcapa MAC (control de acceso al medio) codificada en el campo dirección de destino de la cabecera de trama.

puenteo de ruta en origen (source route bridging). En las LAN, método de puenteo que utiliza el campo de información de direccionamiento de la cabecera MAC (control de acceso al medio) de IEEE 802.5 de una trama para determinar por qué anillos o segmentos de la red en anillo debe transitar la trama. El campo de información de direccionamiento lo inserta el nodo origen en la cabecera MAC. La información de este campo se deriva de los paquetes exploradores generados por el sistema principal origen.

puenteo local (local bridging). Función de un programa puente que permite a un puente individual conectarse a múltiples segmentos de LAN sin utilizar un enlace de telecomunicaciones. Contrástese con *puenteo remoto*.

puenteo remoto (remote bridging). Función de un puente que permite a dos puentes conectar varias LAN utilizando un enlace de telecomunicaciones. Contrástese con *puenteo local*.

puenteo transparente (transparent bridging). En las LAN, método que permite ligar entre sí redes de área local individuales a través del nivel de control de acceso al medio (MAC). El puente transparente almacena las tablas que contienen direcciones MAC para que las tramas vistas por el puente puedan reenviarse a otra LAN, si es que las tablas lo indican así.

puentes en paralelo (parallel bridges). Par de puentes conectados a un mismo segmento de LAN, creándose vías redundantes de acceso al segmento.

puerto (port). (1) Punto de acceso para entrada o salida de datos. (2) Conector de un dispositivo al que se conectan cables de otros dispositivos, como pueden ser estaciones de pantalla e impresoras.
(3) Representación de una conexión física con el hardware de enlace. A veces se llama puerto a un adaptador; sin embargo, un adaptador puede tener más de un puerto. Puede haber uno o varios puertos que estén controlados por un solo proceso DLC. (4) En la serie de protocolos de Internet, número de 16 bits utilizado para establecer comunicación entre TCP o UDP (protocolo de datagrama de usuario) y un protocolo o una aplicación de nivel más alto. Algunos protocolos, como por ejemplo, FTP (protocolo de transferencia de archivos) y SMTP (protocolo simple de transferencia de correo), utilizan el mismo número de puerto conocido públicamente en todas las implementaciones TCP/IP. (5) Abstracción usada por los protocolos de transporte para distinguir entre varios destinos dentro de una máquina de sistema principal. (6) Sinónimo de *zócalo*.

puerto destino (destination port). Adaptador asíncrono de 8 puertos que hace de punto de conexión con un servicio serie.

punto de acceso a servicio (service access point) (SAP). (1) En la arquitectura OSI (interconexión de sistemas abiertos), punto en el que una entidad de una capa proporciona los servicios de esa capa a una entidad de la siguiente capa más alta. (T) (2) Punto lógico que se hace disponible mediante un adaptador y en el que se puede recibir y transmitir información. Un punto de acceso de servicio individual puede hacer de punto de terminación de muchos enlaces.

punto de acceso a servicio destino (destination service access point) (DSAP). En SNA y TCP/IP, dirección lógica que permite a un sistema direccionar datos desde un dispositivo remoto al soporte de comunicaciones adecuado. Contrástese con *punto de acceso a servicio origen (SSAP)*.

punto de acceso a servicio origen (source service access point) (SSAP). En SNA y TCP/IP, dirección lógica que permite a un sistema enviar datos a un dispositivo remoto desde el soporte de comunicaciones adecuado. Contrástese con *punto de acceso a servicio destino (DSAP)*.

punto de control (control point) (CP).
(1) Componente de un nodo APPN o LEN que gestiona los recursos de ese nodo. En un nodo APPN, el CP puede dedicarse a sesiones CP-CP con otros nodos APPN. En un nodo de red APPN, el CP proporciona también servicios a los nodos finales adyacentes de la red APPN. (2) Componente de un nodo que gestiona los recursos de ese nodo y, opcionalmente, proporciona servicios a los demás nodos de la red. Ejemplos de CP son un punto de control de servicios del sistema (SSCP) de un nodo de subárea de tipo 5, un punto de control de nodo de red (NNCP) de un nodo de red APPN, y un punto de control de nodo final (ENCP) de un nodo final APPN o LEN. Los SSCP y NNCP pueden proporcionar servicios a otros nodos.

punto de control de servicios del sistema (SSCP).
Componente de una red de subárea que permite gestionar la configuración, coordinar las peticiones del operador de red y de determinación de problemas y proporcionar servicios de directorio y otros servicios de sesión para los usuarios de la red. Puede haber múltiples SSCP que cooperen entre sí como iguales y que dividan la red en dominios de control, teniendo cada SSCP una relación jerárquica de control con las unidades físicas y las unidades lógicas que hay en su propio dominio.

punto de entrada (entry point) (EP). En SNA, nodo de tipo 2.0, tipo 2.1, tipo 4 o tipo 5 que proporciona soporte de gestión de red distribuida. Envía datos de gestión de red sobre él mismo y sobre los recursos controlados por él a un punto focal a efectos de proceso centralizado, y recibe y ejecuta mandatos iniciados por el punto focal para gestionar y controlar sus recursos.

R

rastreo (trace). (1) Registro de la ejecución de un programa de sistema. Muestra las secuencias de la ejecución de las instrucciones. (A) (2) Para enlaces de datos, registro de las tramas y bytes transmitidos o recibidos.

recepción no preparada (receive not ready) (RNR). En comunicaciones, mandato o respuesta de enlace de datos que indica una condición temporal de incapacidad para aceptar las tramas entrantes.

reconfiguración dinámica (dynamic reconfiguration) (DR). Proceso de cambiar la configuración de red (unidades lógicas y físicas periféricas) sin regenerar todas las tablas de configuración ni desactivar el nodo principal afectado.

recurso (resource). En el conmutador Nways, elemento de hardware o entidad lógica que el programa de control crea. Por ejemplo, los adaptadores, los LIC y las líneas son recursos físicos. Los puntos de control y las conexiones son recursos lógicos.

red (network). (1) Configuración de los dispositivos de proceso de datos y del software conectado para el intercambio de información. (2) Grupo de nodos y los enlaces que los interconectan.

red (network) de comunicaciones avanzadas de igual a igual (APPN). Conjunto de nodos de red interconectados y los correspondientes nodos finales clientes.

red anular (ring network). (1) Red en la que cada uno de los nodos tiene exactamente dos ramas conectadas a él y en la que hay exactamente dos vías entre cada pareja de nodos. (T) (2) Configuración de red en la que los dispositivos están conectados por enlaces de transmisión monodireccionales para formar una vía cerrada.

red APPN (APPN network). Véase *red de comunicaciones avanzadas de igual a igual (APPN)*.

red de área amplia (wide area network) (WAN). (1) Red que proporciona servicios de comunicaciones a un área geográfica de mayor tamaño que la que corresponde a una red de área local o a una red de área metropolitana, y que puede utilizar o proporcionar medios de comunicación públicos. (T) (2) Red de comunicación de datos diseñada para prestar servicio a un área de cientos o miles de kilómetros; por ejemplo, las redes de conmutación de paquetes públicas y privadas y las redes telefónicas nacionales. (3) Contrástese con *red de área local (LAN)* y *red de área metropolitana (MAN)*.

red de área local (local area network) (LAN). (1) Red de sistemas ubicada en el local de un usuario, en un área limitada geográficamente. La comunicación dentro de una red de área local no está sujeta a normativas externas; sin embargo, la comunicación a través de la frontera de la LAN sí puede estar sujeta a algún tipo de normativas. (T) (2) Red en la que un conjunto de dispositivos están conectados entre sí para comunicarse y que pueden conectarse a una red de mayor tamaño. (3) Véase también *Ethernet* y *red en anillo*. (4) Contrástese con *red de área metropolitana (MAN)* y *red de área amplia (WAN)*.

red de área metropolitana (metropolitan area network) (MAN). Red, formada por la interconexión de dos o más redes, que puede operar a una velocidad superior a las redes interconectadas, atravesar los límites administrativos y utilizar múltiples métodos de acceso. (T) Contrástese con *red de área local (LAN)* y *red de área amplia (WAN)*.

red de clase A (class A network). En las comunicaciones Internet, red en la que el bit de orden superior (el más significativo) de la dirección IP se establece en 0 y el ID de sistema principal ocupa los tres octetos de orden inferior.

red de clase B (class B network). En las comunicaciones Internet, red en la que los dos bits de orden superior (el más significativo y el que le sigue) de la dirección IP se establecen en 1 y 0, respectivamente, y el ID de sistema principal ocupa los dos octetos de orden inferior.

red de entrada limitada (low-entry networking) (LEN). Posibilidad que tienen los nodos de conectarse directamente entre sí mediante protocolos básicos de igual a igual para dar soporte a sesiones múltiples y paralelas entre unidades lógicas.

red digital de servicios integrados (integrated services digital network) RDSI (ISDN). Red digital de telecomunicaciones entre extremos que da soporte a múltiples servicios, incluidos, sin limitarse a ellos, los de voz y datos.

Nota: Las RDSI se utilizan en las arquitecturas de red de uso público y privado.

red en anillo (token ring). (1) Según la IEEE 802.5, tecnología de red que controla el acceso al medio pasando un testigo (paquete o trama especial) entre las estaciones conectadas por el medio. (2) Red o IEEE 802.5 con topología de anillo que pasa testigos de una a otra estación (nodo) del anillo de conexión. (3) Véase también *red de área local (LAN)*.

red en anillo (token-ring network). (1) Red en anillo que permite la transmisión de datos monodireccional entre estaciones de datos, mediante un procedimiento de paso de testigo, de tal forma que los datos transmitidos vuelven a la estación transmisora. (T) (2) Red que utiliza la topología de anillo, en la que se pasan testigos de nodo a nodo, en circuito. Un nodo que esté preparado para enviar puede capturar el testigo e insertar datos para su transmisión.

red óptica síncrona (synchronous optical network) (SONET). Estándar en los Estados Unidos para transmitir información digital a través de interfaces ópticas. Tiene estrecha relación con la recomendación SDH (jerarquía digital síncrona).

red troncal (backbone network). Red central a la que se conectan redes de menor tamaño, normalmente de velocidad más baja. La red troncal suele tener una capacidad mucho más elevada que las redes a las que ayuda a interconectarse; también puede ser una red de área amplia (WAN) como, por ejemplo, una red pública de datagrama de paquetes conmutados.

red troncal (backbone). (1) En una configuración en anillo multipuente de una red de área local, enlace de alta velocidad al que se conectan los anillos por medio de puentes o direccionadores. Una red troncal puede configurarse como bus o como anillo. (2) En una red de área amplia, enlace de alta velocidad al que se conectan nodos o equipos de conmutación de datos (DSE).

reensamblaje (reassembly). En comunicaciones, proceso de volver a reunir los paquetes segmentados después de que se han recibido.

remoto (remote). (1) Dícese de un sistema, un programa o un dispositivo al que se accede mediante una línea de telecomunicaciones. (2) Sinónimo de *conectado por enlace*. (3) Contrástese con *local*.

resolución de direcciones (address resolution). (1) Método de correlación entre las direcciones de la capa de red y las direcciones específicas de medio. (2) Véase también *Protocolo de resolución de direcciones (Address Resolution Protocol) (ARP)* y *Protocolo de resolución de direcciones de AppleTalk (AppleTalk Address Resolution Protocol) (AARP)*.

resolución de nombres (name resolution). En las comunicaciones Internet, proceso de correlacionar un nombre de máquina con la correspondiente dirección IP (protocolo Internet). Véase también *sistema de nombres de dominio (DNS)*.

respuesta de excepción (exception response) (ER). En SNA, protocolo solicitado en el campo forma-de-respuesta-solicitada de una cabecera de petición que insta al receptor a devolver una respuesta sólo si la petición es inaceptable tal como se ha recibido o si no puede procesarse; es decir, puede devolverse una respuesta negativa, pero no una positiva. Contrástese con *respuesta definitiva* y *sin respuesta*.

restablecimiento (reset). En un circuito virtual, reinicialización del control de flujo de datos. Al restablecer, se eliminan todos los datos de tránsito.

ritmo (pacing). (1) Técnica mediante la que un componente receptor controla la velocidad de transmisión de un componente emisor para evitar el desbordamiento o la congestión. (2) Véase también *control de flujo*, *ritmo de recepción*, *ritmo de envío*, *ritmo a nivel de sesión* y *ritmo de ruta virtual (VR)*.

rlogin (inicio de sesión remoto). Servicio, ofrecido por los sistemas basados en UNIX de Berkeley, que permite a los usuarios autorizados de una máquina conectarse a otros sistemas UNIX a lo largo de un conjunto de redes e interactuar como si sus terminales estuviesen conectados directamente. El software de rlogin pasa información acerca del entorno del usuario (por ejemplo, el tipo de terminal) a la máquina remota.

rsh. Variante del mandato rlogin que invoca un intérprete de mandato en una máquina UNIX remota y pasa los argumentos de línea de mandatos al intérprete de mandato, saltándose completamente el paso de inicio de sesión.

ruta (route). (1) Secuencia ordenada de nodos y grupos de transmisión (TG) que representan una vía desde un nodo origen a un nodo destino, por la que circula el tráfico intercambiado entre ellos. (2) Vía que el tráfico de red utiliza para ir desde el origen al destino.

ruta estática (static route). Ruta entre sistemas principales, redes, o ambas cosas, que se entra manualmente en una tabla de direccionamiento.

ruta explícita (explicit route) (ER). En SNA, serie de uno o más grupos de transmisión que conecta dos nodos de subárea. La ruta explícita se identifica mediante una dirección de subárea origen, una dirección de subárea destino, un número de ruta explícita y un número de ruta explícita inversa. Contrástese con *ruta virtual (VR)*.

ruta virtual (virtual route) (VR). (1) En SNA, (a) conexión lógica entre dos nodos de subárea que adquiere el aspecto físico de una ruta explícita determinada o (b) conexión lógica que está enteramente contenida en un nodo de subárea para sesiones intranodo. Una ruta virtual entre distintos nodos de subárea impone una prioridad de transmisión en la ruta explícita subyacente, proporciona el control de flujo mediante el ritmo de ruta virtual, y suministra la integridad de datos mediante la secuencia de numeración de las unidades de información de vía (PIU). (2) Contrástese con *ruta explícita (ER)*. Véase también *vía* y *extensión de ruta (REX)*.

rutina de carga (bootstrap). (1) Secuencia de instrucciones cuya ejecución hace que se carguen y ejecuten más instrucciones hasta que se haya almacenado todo el programa de sistema. (T) (2) Técnica o dispositivo diseñado para autocargarse con el estado deseado por medio de su propia acción; por ejemplo, una rutina de máquina cuyas primeras instrucciones sean suficientes para cargar en el sistema lo que queda de sí misma desde un dispositivo de entrada. (A)

S

salto (hop). (1) En APPN, parte de una ruta que no tiene ningún nodo intermedio. Consta de un solo grupo de transmisión que conecta nodos adyacentes. (2) Para la capa de direccionamiento, distancia lógica entre dos nodos de una red.

SAP. Véase punto de acceso a servicio.

segmentación (segmenting). En OSI, función realizada por una capa para hacer que una unidad de datos de

protocolo (PDU) de la capa soportada se correlacione con múltiples PDU.

segmento (segment). (1) Sección de cable entre componentes o dispositivos. Un segmento puede constar de un solo cable provisional, de varios cables provisionales conectados, o bien de una combinación de un cable de fachada y varios cables provisionales conectados. (2) En las comunicaciones Internet, unidad de transferencia entre funciones TCP de distintas máquinas. Cada segmento contiene campos de control y de datos; para validar los datos recibidos, se identifican la posición de la corriente de bytes actual y los bytes de datos reales junto con una suma de comprobación.

segmento de anillo (ring segment). Sección de un anillo que se puede aislar (desenchufando conectores) del resto del anillo. Véase *segmento de LAN*.

segmento de LAN (LAN segment). (1) Cualquier parte de una LAN (por ejemplo, un bus o un anillo) que puede operar de forma independiente, pero que está conectado a otras partes de la red por medio de puentes. (2) Una red de anillo o bus sin ningún puente.

servicio de directorio (directory service) (DS). Elemento de servicio de la aplicación que hace que los nombres simbólicos utilizados por los procesos de la aplicación se conviertan a las direcciones de red completas utilizadas en un entorno OSI. (T)

servicios de directorio (directory services) (DS). Componente de punto de control de un nodo APPN que mantiene el conocimiento de la ubicación de los recursos de red.

servicios de gestión de punto de control (control point management services) (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, la gestión de rendimiento y contabilidad, la gestión de cambios y la gestión de configuración. Entre las posibilidades proporcionadas por los CPMS se cuentan el envío de peticiones a los servicios de gestión de unidades físicas (PUMS) para probar los recursos del sistema, la recogida de información estadística (por ejemplo, datos de rendimiento y errores) de los PUMS acerca de los recursos del sistema, así como el análisis y la presentación de los resultados de prueba y de la información estadística recogida acerca de los recursos del sistema. Las responsabilidades de análisis y presentación para la determinación de problemas y la supervisión de rendimiento pueden distribuirse entre varios CPMS.

servicios de gestión SNA (SNA management services) (SNA/MS). Servicios proporcionados para ayudar a gestionar las redes SNA.

servidor (server). Unidad funcional que proporciona servicios compartidos a las estaciones de trabajo a través de una red; por ejemplo, un servidor de archivos, un servidor de impresión o un servidor de correo. (T)

servidor de acceso de red (Network Access Server) (NAS). Dispositivo que proporciona a los usuarios acceso temporal y a petición a la red. Este acceso se realiza punto a punto mediante líneas PSTN o RDSI.

servidor de informe de configuración (configuration report server) (CRS). En el programa IBM Token-Ring Network Bridge, servidor que acepta mandatos de un LNM (LAN Network Manager) para obtener información de estación, establecer parámetros de estación y eliminar estaciones del anillo. Además, este servidor recoge y reenvía informes de configuración generados por las estaciones del anillo. Los informes de configuración incluyen los de los nuevos supervisores activos y los de la estación contigua activa de donde proceden los datos (NAUN).

servidor de nombres (name server). En la serie de protocolos de Internet, sinónimo de *servidor de nombres de dominio*.

servidor de nombres de dominio (domain name server). En la serie de protocolos de Internet, programa servidor que proporciona la conversión de nombre a dirección, correlacionando los nombres de dominio con las direcciones IP. Sinónimo con *servidor de nombres*.

servidor de puente de LAN (LAN bridge server) (LBS). En el programa IBM Token-Ring Network Bridge, servidor que mantiene información estadística acerca de las tramas reenviadas entre dos o más anillos (a través de un puente). LBS envía estas estadísticas a los gestores de LAN apropiados mediante los mecanismos de información de LAN (LRM).

sesión (session). (1) En la arquitectura de redes y a efectos de comunicación de datos entre unidades funcionales, todas las actividades que tienen lugar durante el establecimiento, el mantenimiento y la liberación de la conexión. (T) (2) Conexión lógica entre dos unidades accesibles de red (NAU) que, según se solicite, puede activarse, adaptarse para proporcionar los diversos protocolos y desactivarse. Cada sesión se identifica inequívocamente en una cabecera de transmisión (TH) que acompaña a las transmisiones que se intercambien durante esa sesión.

síncrono (synchronous). (1) Dícese de dos o más procesos que dependen de que se produzcan sucesos específicos, tales como señales de sincronización común. (T) (2) Que se produce con una relación temporal regular o predecible.

sintaxis abstracta (abstract syntax). Especificación de datos que incluye todas las distinciones necesarias de las transmisiones de datos, pero que omite (abstrae) otros detalles, como los que dependen de las arquitecturas específicas de PC. Véase también *notación de sintaxis abstracta 1 (ASN.1)* y *reglas básicas de codificación (BER)*.

sistema (system). En proceso de datos, conjunto de personas, máquinas y métodos organizados para lograr una serie de funciones específicas. (I) (A)

sistema autónomo (autonomous system). En TCP/IP, grupo de redes y direccionadores bajo una autoridad administrativa. Estas redes y direccionadores cooperan estrechamente para propagar entre sí información de accesibilidad (y direccionamiento) de red utilizando un protocolo de pasarela interior de su elección.

sistema de conjunto reducido de instrucciones (reduced instruction-set computer) (RISC). Sistema que utiliza un conjunto pequeño y simplificado de las instrucciones usadas con frecuencia para ejecución rápida.

sistema de nombres de dominio (Domain Name System) (DNS). En la serie de protocolos de Internet, sistema de base de datos distribuido que se utiliza para correlacionar los nombres de dominio con las direcciones IP.

sistema principal (host). En la serie de protocolos de Internet, sistema final. Puede ser cualquier estación de trabajo; no hace falta que sea un sistema central.

sistemas de redes Xerox (Xerox Network Systems) (XNS). Serie de protocolos interredes desarrollados por Xerox Corporation. Aunque se parece a los protocolos TCP/IP, XNS utiliza otros formatos de paquete y una terminología distinta. Véase también *intercambio de paquetes interredes (IPX)*.

socket. (1) Punto final de la comunicación entre procesos o programas de aplicación. (2) Según Distribución de Software de la Universidad de Berkeley (llamada comúnmente UNIX de Berkeley o UNIX BSD), California, abstracción que hace de punto final en la comunicación entre procesos o aplicaciones.

sonda de paquetes InterNet (packet internet groper) (PING). (1) En las comunicaciones Internet, programa utilizado en las redes TCP/IP que permite probar la capacidad de acceder a los destinos enviándoles una petición de eco ICMP (protocolo de mensaje de control Internet) y esperando una respuesta. (2) En comunicaciones, prueba de accesibilidad.

sondeo (polling). (1) En una conexión multipunto o en una conexión punto a punto, proceso por el que se invita individualmente a las estaciones a transmitir. (I) (2) Interrogación que se hace a los dispositivos con objeto de evitar contiendas, determinar el estado operativo o determinar la disponibilidad para enviar o recibir datos. (A)

soporte de dominio múltiple (multiple-domain support) (MDS). Técnica para transportar datos de servicios de gestión entre conjuntos de funciones de servicios de gestión a través de sesiones LU-LU y CP-CP. Véase también *unidad de mensaje para soporte de dominio múltiple (MDS-MU)*.

StreetTalk. En VINES (VIrtual NEtworking System), sistema exclusivo de nombres y direcciones a escala de red que permite a los usuarios localizar y acceder a los recursos de la red sin conocer la topología de ésta. Véase también *protocolo de control de Internet (ICP)* y *protocolo de actualización de direccionamiento (RTP)*.

subárea (subarea). Parte de la red SNA que consta de un nodo de subárea, nodos periféricos conectados y recursos asociados. Dentro de un nodo de subárea, todas las unidades accesibles de red (NAU), los enlaces, y las estaciones de enlace adyacentes (de nodos periféricos conectados o nodos de subárea) que son direccionables dentro de la subárea comparten una dirección de subárea común y tienen direcciones de elemento diferenciadas.

subcapa de control de acceso al medio (MAC sublayer). En una red de área local, la 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 topología y utiliza los servicios de una capa física para proporcionar servicios a la subcapa de control de enlace lógico. (T)

subred (subnet). (1) En TCP/IP, parte de una red que se identifica mediante una parte de la dirección IP. (2) Sinónimo de *subred (subnetwork)*.

subred (subnetwork). (1) Cualquier grupo de nodos que tienen en común un conjunto de características como, por ejemplo, el mismo ID de red. (2) Sinónimo con *subred (subnet)*.

subsistema (subsystem). Sistema secundario o subordinado que, en general, puede operar ya sea independientemente de un sistema de control o bien asíncronamente con un sistema de control. (T)

suma de comprobación (checksum). (1) Suma de un grupo de datos asociados al grupo y usados a efectos de comprobación. (T) (2) En detección de errores, función de todos los bits de un bloque. Si la suma escrita no concuerda con la calculada, se indica un error. (3) En un disquete, datos escritos en un sector a efectos de detección de errores; una suma de comprobación calculada que no se corresponda con la suma de comprobación de los datos escritos en el sector, indica un sector defectuoso. Los datos son ya sea numéricos o bien otras series de caracteres consideradas como numéricas a la hora de calcular la suma de comprobación.

supervisor - supervisar (monitor). (1) Dispositivo que observa y registra, para el análisis, actividades seleccionadas de un sistema de proceso de datos. Puede utilizarse para indicar desviaciones significativas de la norma, o para determinar niveles de utilización de determinadas unidades funcionales. (T) (2) Software o hardware que observa, inspecciona, controla o verifica las operaciones de un sistema. (A) (3) Función requerida para iniciar la transmisión de un testigo en un anillo y para proporcionar recuperación de errores de software en caso de testigos perdidos, tramas que circulen u otras dificultades. Esta función está presente en todas las estaciones del anillo.

supervisor activo (active monitor). En una red en anillo, función que realiza en cualquier momento una

estación del anillo y que inicia la transmisión del testigo y proporciona servicios de recuperación de errores de testigo. Cualquier adaptador activo de la red tiene la capacidad de proporcionar la función de supervisor activo si falla el supervisor activo actual.

SYNTAX. En el protocolo simple de gestión de red (SNMP), cláusula del módulo MIB que define la estructura de datos abstracta que corresponde a un objeto gestionado.

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 2.048 Mbps.

tabla de correlación de direcciones (address mapping table) (AMT). Tabla, mantenida en el direccionador AppleTalk, que proporciona una correlación actualizada entre las direcciones de los nodos y las direcciones de hardware.

tabla de direccionamiento (routing table). Conjunto de rutas utilizado para el reenvío directo de datagramas o para establecer una conexión. La información se pasa entre direccionadores para identificar la topología de la red y la viabilidad de los destinos.

tabla de información de zonas (zone information table) (ZIT). Listado de las correlaciones entre los números de red y los nombres de zona asociados del conjunto de redes. Este listado lo mantiene cada uno de los direccionadores de un conjunto de redes AppleTalk.

TCP/IP. (1) Protocolo de control de transmisión/protocolo Internet. (2) Protocolo de interconexión de sistemas al estilo UNIX y/o basado en Ethernet desarrollado originalmente por el Departamento de Defensa de los Estados Unidos. TCP/IP facilitó ARPANET (Advanced Research Projects Agency Network), una red de investigación de paquetes conmutados en la que la capa 4 era TCP y la capa 3, IP.

Telnet. En la serie de protocolos de Internet, protocolo que proporciona un servicio de conexión de terminal remoto. Permite a los usuarios de un sistema principal conectarse a un sistema principal remoto e interactuar como si fuesen usuarios de terminal conectado directamente de ese sistema principal.

terminal de datos preparado (data terminal ready) (DTR). Señal que se envía al módem con el protocolo EIA 232.

testigo (token). (1) En una red de área local, símbolo de la autorización que se pasa sucesivamente de una a otra estación de datos para indicar la estación que controla temporalmente el medio de transmisión. Cada estación de datos tiene la oportunidad de adquirir y utilizar el testigo para controlar el medio. El testigo consiste en un determinado mensaje o patrón de bits que signifique el permiso para transmitir. (T) (2) En las LAN, secuencia de bits que se pasa de un a otro dispositivo a lo largo del medio de transmisión. Cuando el testigo tiene datos añadidos a él, pasa a ser una trama.

tiempo de espera (timeout). (1) Suceso que se produce al final de un tiempo predeterminado, contado a partir del momento en que se produjo otro suceso especificado. (I) (2) Intervalo de tiempo asignado para que se produzcan ciertas operaciones; por ejemplo, la respuesta al sondeo o al direccionamiento antes de que la operación del sistema se interrumpa y deba reiniciarse.

tiempo de vida (time to live) (TTL). Técnica que los protocolos de entrega del mejor esfuerzo utilizan para inhibir la repetición de paquetes en un bucle sin fin. El paquete queda descartado si el contador TTL se hace igual a 0.

topología (topology). En comunicaciones, disposición física o lógica de los nodos de una red, especialmente las relaciones entre los nodos y los enlaces que hay entre ellos.

trama (frame). (1) En la arquitectura OSI (interconexión de sistemas abiertos), estructura de datos perteneciente a un área determinada del conocimiento y que consta de ranuras que pueden aceptar los valores de atributos específicos y a partir de la cual se pueden sacar conclusiones mediante conexiones procedimentales adecuadas. (T) (2) Unidad de transmisión de algunas redes de área local, entre ellas la red en anillo de IBM. Incluye delimitadores, caracteres de control, información y caracteres de comprobación. (3) En SDLC, vehículo de todos y cada uno de los mandatos y respuestas, así como de toda la información que se transmite mediante los procedimientos SDLC.

trama de información (information (I) frame). Trama en formato I utilizada para la transferencia de información numerada.

trama exploradora (explorer frame). Véase *paquete explorador*.

trama I (I-frame). Trama de información.

transceptor (transmisor-receptor) (transceiver). En las LAN, dispositivo físico que conecta una interfaz de sistema principal a una red de área local, como puede ser Ethernet. Los transceptores de Ethernet contienen la electrónica que aplica las señales al cable y que detecta las colisiones.

transporte de vector de gestión de red (network management vector transport) (NMVT). Unidad de petición/respuesta (RU) de los servicios de gestión que fluye a través de una sesión activa entre los servicios de gestión de unidad física y los servicios de gestión de punto de control (sesión SSCP-PU).

U

umbral (threshold). (1) En los programas de puente IBM, valor establecido para el número máximo de tramas que no se reenvían a través de un puente debido a errores, antes de que se cuente una aparición de "umbral excedido" y ésta se indique a los programas de gestión de red. (2) Valor inicial a partir del que un contador va disminuyendo hasta 0, o valor hasta el que un contador va aumentando o disminuyendo desde un valor inicial.

unidad accesible de red (network accessible unit) (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 vía. Sinónimo con *unidad direccionable de red*.

unidad de datos de protocolo (protocol data unit) (PDU). Unidad de datos especificada en un protocolo de una capa determinada y que consta de la información de control de protocolo de esa capa y, posiblemente, de datos de usuario correspondientes a esa capa. (T)

unidad de datos del protocolo de control de enlace lógico (logical link control (LLC) protocol data unit). Unidad de información intercambiada entre estaciones de enlace de distintos nodos. La unidad de datos de protocolo LLC contiene un punto de acceso a servicio destino (DSAP), un punto de acceso a servicio origen (SSAP), un campo de control y datos de usuario.

unidad de información de vía (path information unit) (PIU). Unidad de mensaje que consta de una sola cabecera de transmisión (TH), o de una cabecera TH seguida de una unidad de información básica (BIU) o de un segmento BIU.

unidad de mensaje para soporte de dominio múltiple (multiple-domain support message unit) (MDS-MU). Unidad de mensaje que contiene datos de servicios de gestión y que fluye entre los conjuntos de funciones de servicios de gestión a través de las sesiones LU-LU y CP-CP utilizadas por el soporte de dominio múltiple. Esta unidad de mensaje, como también los datos de servicios de gestión reales contenidos en ella, tiene el formato de corriente general de datos (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 servicio de canal (channel service unit) (CSU). Unidad que proporciona el intercambio de información con una red digital. La CSU proporciona las siguientes funciones: condicionamiento (o igualación) de línea, que hace que el rendimiento de la señal se mantenga coherente en todo el ancho de banda del canal; remodelado de señal, que constituye la corriente de de impulsos binarios; comprobación 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 (data service unit) (DSU). Dispositivo que proporciona directamente al equipo terminal de datos una interfaz de servicio de datos digitales. La DSU proporciona la igualación de bucle, posibilidades de comprobación local y remota, y una interfaz EIA/CCITT estándar.

unidad de servicios de gestión de punto de control (control point management services unit) (CP-MSU). Unidad de mensaje que contiene los datos de servicios de gestión y que fluye entre los conjuntos de funciones de servicios de gestión. Esta unidad de mensaje tiene el formato de corriente general de datos (GDS). Véase también *unidad de servicios de gestión (MSU)* y *transporte de vector de gestión de red (NMVT)*.

unidad de transmisión básica (basic transmission unit) (BTU). En SNA, unidad de información de datos y de control que se pasa entre componentes de control de vía. Una BTU puede constar de una o varias PIU (unidad de información de vía).

unidad de transmisión máxima (maximum transmission unit) (MTU). En las LAN, la mayor unidad posible de datos que puede enviarse en un determinado medio físico y en una sola trama. Por ejemplo, la MTU de Ethernet es de 1500 bytes.

unidad direccionable de red (network addressable unit) (NAU). Sinónimo de *unidad accesible de red*.

unidad EIA (EIA unit). Unidad de medida, establecida por Electronic Industries Association, que equivale a 44,45 milímetros (1,75 pulgadas).

unidad física (physical unit) (PU). (1) Componente que gestiona y supervisa los recursos (tales como los enlaces conectados y las estaciones de enlace adyacentes) asociados a un nodo, según lo solicite un SSCP por medio de una sesión SSCP-PU. Un SSCP activa una sesión con la unidad física para gestionar indirectamente, mediante la PU, recursos del nodo, tales como los enlaces conectados. Este término sólo es aplicable a los nodos de tipo 2.0, de tipo 4 y de tipo 5. (2) Véase también *PU periférica* y *PU de subárea*.

unidad lógica (logical unit) (LU). Tipo de unidad de red accesible que permite a los usuarios obtener acceso a los recursos de red y comunicarse entre sí.

Unión Internacional de Telecomunicaciones (International Telecommunication Union) (ITU). Organismo de las Naciones Unidas especializado en telecomunicaciones y establecido para proporcionar procedimientos y prácticas de comunicaciones estandarizadas, incluyendo la asignación de frecuencias y la reglamentación de radio a escala mundial.

usurpación (spoofing). Para los enlaces de datos, técnica en la que un nodo intermedio en nombre del destino final emite un acuse de recibo y procesa un protocolo iniciado desde una estación final. Por ejemplo, en la conmutación de enlace de datos de IBM 6611, las tramas SNA se encapsulan en paquetes TCP/IP para el transporte a través de una red de área amplia no SNA, se desempaquetan mediante otro IBM

6611, y se pasan al destino final. La usurpación tiene la ventaja de que puede impedir que se excedan los tiempos de espera en las sesiones extremo a extremo.

V

V.24. En la comunicación de datos, especificación del CCITT que define la lista de definiciones para intercambiar circuitos entre el DTE (equipo terminal de datos) y el DCE (equipo de terminación de circuito de datos).

V.25. En la comunicación de datos, especificación del CCITT que define el equipo de respuesta automática y el equipo paralelo de llamada automática en la red telefónica general conmutada, incluyendo procedimientos para inhabilitar dispositivos controlados por eco para establecer llamadas tanto manual como automáticamente.

V.34. Recomendación de ITU-T para la comunicación por módem a través de canales estándar de 33,6 Kbps (y más lentos) de grado de voz comercialmente disponibles.

V.35. En la comunicación de datos, especificación del CCITT que define la lista de definiciones para intercambiar circuitos entre el DTE (equipo terminal de datos) y el DCE (equipo de terminación de circuito de datos) en diversas velocidades de datos.

V.36. En la comunicación de datos, especificación del CCITT que define la lista de definiciones para intercambiar circuitos entre el DTE (equipo terminal de datos) y el DCE (equipo de terminación de circuito de datos) con las velocidades de 48, 56, 64 o 72 kilobits por segundo.

variable de corriente general de datos (GDS). Tipo de subestructura de RU que va precedida de un identificador y un campo de longitud y que incluye ya sea datos de aplicación, datos de control de usuario o datos de control definidos por SNA.

variable MIB (MIB variable). En el protocolo simple de gestión de red (SNMP), instancia específica de datos definida en un módulo MIB. Sinónimo con *objeto MIB*.

vector de control de selección de ruta (Route Selection control vector) (RSCV). Vector de control que describe una ruta en una red APPN. RSCV consta de una secuencia ordenada de vectores de control que identifican los TG y los nodos que constituyen la vía desde un nodo origen hasta un nodo destino.

velocidad de transferencia de datos (data transfer rate). Número promedio de bits, caracteres o bloques por unidad de tiempo que se pasa entre equipos que se corresponden 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 en correspondencia; por ejemplo, módems, equipo intermedio, o fuente y sumidero.

versión (version). Programa bajo licencia por separado que suele tener código nuevo o funciones nuevas significativos.

vía (path). (1) En una red, cualquier ruta entre cualquier pareja de nodos. Una vía puede incluir más de una rama. (T) (2) Serie de componentes de red de transporte (control de vía y control de enlace de datos) que la información intercambiada atraviesa 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, el enlazamiento virtual permite que todos los dispositivos y servicios parezcan estar directamente conectados entre sí, cuando en realidad pueden estar a miles de kilómetros de distancia. Véase también *StreetTalk*.

vista de MIB (MIB view). En el protocolo simple de gestión de red (SNMP), conjunto de objetos gestionados que el agente conoce y que es visible para una determinada comunidad.

vuelco - volcar (dump). (1) Datos que se han volcado. (T) (2) Copiar el contenido de todo o parte del almacenamiento virtual con objeto de recoger información de errores.

X

X.21. Recomendación CCITT (Comité Consultivo Internacional de Telegrafía y Telefonía) para una interfaz de uso general entre el equipo terminal de datos y el equipo de terminación de circuito de datos para operaciones síncronas en una red de datos pública.

X.25. (1) Recomendación CCITT (Comité Consultivo Internacional de Telegrafía y Telefonía) para la interfaz entre el equipo terminal de datos y las redes de datos de paquetes conmutados. (2) Véase también *conmutación de paquetes*.

Z

zona (zone). En las redes AppleTalk, subconjunto de nodos de un conjunto de redes.

Índice

A

acceder al indicador de configuración de la autenticación 253
acceso a Host On-Demand Client Cache 155
acceso a la Antememoria de servidor Web 208
ACE/Sever
  autenticación 250
activate
  mandato de configuración de Host On-Demand Client Cache 156
  mandato de configuración de la Antememoria de servidor Web 208
  mandato de supervisión de Host On-Demand Client Cache 159
  mandato de supervisión de la Antememoria de servidor Web 216
activate-ip-precedence-filtering
  mandato de configuración de la reserva de ancho de banda 30
adaptador de voz
  configuración 583, 587
  utilización 579
  visión general 580
add
  mandato de actualización del filtrado MAC 64
  mandato de configuración de Host On-Demand Client Cache 156
  mandato de configuración de la Antememoria de servidor Web 208
  mandato de configuración de la característica de voz 588
  mandato de configuración de la restauración de WAN 78
  mandato de configuración de la TSF 559
  mandatos de configuración del servidor DHCP 510
add server
  mandato de configuración de seguridad IP 355
add tunnel
  mandato de configuración de seguridad IP 359
add-circuit-class
  mandato de configuración de la reserva de ancho de banda 31
add-class
  mandato de configuración de la reserva de ancho de banda 31
agrupaciones de módems
  configuración 457
AH 338
algoritmos de la seguridad IP (IPv4) 358
algoritmos para seguridad IP (IPv6) 370
almacenamiento en antememoria 167
Antememoria de servidor Web
  definición de un cluster 117
Antememoria escalable de alta disponibilidad 172
asesores
  para network dispatcher 106
asociación de seguridad (SA) 340
assign
  mandato de configuración de la reserva de ancho de banda 33
assign-circuit
  mandato de configuración de la reserva de ancho de banda 36
atributos de la seguridad AAA remota 605
  palabras clave 605
  radius 605
  TACACS 606
atributos de la seguridad AAA, remota 605
attach
  mandato de configuración del filtrado MAC 60
attributos, de la seguridad AAA remota 605
autenticación 245, 253
  mandatos de configuración 253
  seguridad 245
  utilización de la identificación de seguridad 250
    limitaciones 251
Autenticación del gestor de control de antememoria externa 176
autorización
  seguridad 245

C

cabecera de autenticación (AH) 338
calls
  mandato de supervisión del adaptador de voz 601
características
  Reserva de ancho de banda 1
carga útil de seguridad de encapsulación (ESP) 339
cert-load
  mandato de supervisión de PKI (IPv4) 378
cert-req
  mandato de supervisión de PKI (IPv4) 378
cert-save
  mandato de supervisión de PKI (IPv4) 379
certificado
  obtención 354
cifrado
  configurar 271
    para Frame Relay 274
  configurar ECP
    para PPP 271
  configurar MPPE
    para PPP 273
  Frame Relay 271
  PPP 271
  supervisar
    para Frame Relay 274
    para PPP 272
  supervisar MPPE
    para PPP 273
Cifrado de punto a punto de MS
  configurar 271
  para PPP 272
circuit
  mandato de configuración de la reserva de ancho de banda 37
  mandato de supervisión de la reserva de ancho de banda 51

circuito de establecimiento de conexión
valores por omisión de parámetros
para interfaces de establecimiento de conexión de entrada 454
claves 353
para seguridad IP (IPv4), configuración 359
para seguridad IP (IPv6), configuración 370
claves de cifrado 353
para seguridad IP (IPv4), configuración 359
clear
mandato de supervisión de Host On-Demand Client Cache 160
mandato de supervisión de la Antememoria de servidor Web 216
mandato de supervisión de la reserva de ancho de banda 52
mandato de supervisión del filtrado MAC 67
mandato de supervisión del VCRM 576
mandatos de supervisión de la restauración de WAN 86
clear-block
mandato de configuración de la reserva de ancho de banda 38
clear-circuit-class
mandato de supervisión de la reserva de ancho de banda 52
códigos de retorno 199
códigos de retorno y sus descripciones 199
colas de prioridad
descripción 5
compresión
visión general
Frame Relay 231
PPP 231
compresión de datos
conceptos 231
consideraciones 234
carga de la CPU 234
compresión en la capa de enlace 236
contenido de los datos 236
ocupación de la memoria 235
diccionario de datos
definición de 232
compresión de datos *(continuación)*
historia
definición de 232
nociones básicas 232
para enlaces Frame Relay 239
configuración 239
supervisión 241
sesiones de compresión
definición de 235
visión general 231
configuración 353
acceder al indicador de autenticación 253
compresión de datos para enlaces Frame Relay 239
Compresión de datos para enlaces PPP 236
diffserv 395
infraestructura de claves públicas 354
intercambio de claves en Internet 353
interfaz de establecimiento de conexión de entrada 453
interfaz de establecimiento de conexión de salida 456
protocolos L2 417
Restauración de WAN 77
seguridad IP (IPv6) 369
seguridad IP manual (IPv4) 358
túnel manual (IPv4) 368
túnel manual (IPv6) 371
configuración y supervisión de la Antememoria de servidor Web 201
configurar
cifrado 271
para Frame Relay 274
Cifrado de punto a punto de MS 271
ECP, cifrado
para PPP 271
LDAP 311
MPPE
para PPP 273
políticas 311
contabilidad
seguridad 245
conversión de direcciones de red
configuración 441
mandatos de supervisión 448
conversión de direcciones de red (NAT)
Véase también ?
utilización 433
Conversión de puertos y direcciones de red (NAPT)
Conversión de puertos y direcciones de red (NAPT) *(continuación)*
utilización 434
correlaciones de direcciones estáticas 435
counters
mandato de supervisión de la reserva de ancho de banda 52
counters-circuit-class
mandato de supervisión de la reserva de ancho de banda 53
create
mandatos de configuración del filtrado MAC 60
create-super-class
mandato de configuración de la reserva de ancho de banda 38

CH

change
mandato de conversión de direcciones de red 442
mandato NAT 442
mandatos de configuración del servidor DHCP 516
change server
mandato de configuración de seguridad IP 355
change tunnel
mandato de configuración de seguridad IP 364
mandato de supervisión de seguridad IP 381
change-circuit-class
mandato de configuración de la reserva de ancho de banda 37
change-class
mandato de configuración de la reserva de ancho de banda 37

D

deactivate-ip-precedence-filtering
mandato de configuración de la reserva de ancho de banda 39
deassign
mandato de configuración de la reserva de ancho de banda 39

deassign-circuit
mandato de configuración de la reserva de ancho de banda 39
default
mandato de configuración del filtrado MAC 60
default-circuit-class
mandato de configuración de la reserva de ancho de banda 39
default-class
mandato de configuración de la reserva de ancho de banda 40
definición de un cluster
Host On-Demand Client Cache 118
del-circuit-class
mandato de configuración de la reserva de ancho de banda 40
del-class
mandato de configuración de la reserva de ancho de banda 40
delete
mandato de actualización del filtrado MAC 65
mandato de configuración de Host On-Demand Client Cache 156
mandato de configuración de la Antememoria de servidor Web 209
mandato de configuración de la característica de voz 591
mandato de configuración de la TSF 565
mandato de configuración del filtrado MAC 61
mandato de conversión de direcciones de red 442
mandato de supervisión de Host On-Demand Client Cache 160
mandato de supervisión de la Antememoria de servidor Web 217
mandato de supervisión de seguridad IP 376
mandato NAT 442
mandatos de configuración del servidor DHCP 521
delete certificate
mandato de configuración de seguridad IP 356
delete private-key
mandato de configuración de seguridad IP 356
delete server
mandato de configuración de seguridad IP 356
delete tunnel
mandato de configuración de seguridad IP (IPv4) 365
mandato de supervisión de seguridad IP 382
delete-file
mandato de supervisión de la TSF 569
detach
mandato de configuración del filtrado MAC 61
diagrama de red
IP, túnel de seguridad 344
dial-in access server
direcciones IP proporcionadas por el servidor 458
métodos de asignación de direcciones IP 459
DIALs
agrupaciones de módems
configuración 457
definición 451
interfaz de establecimiento de conexión de entrada
configuración 453
interfaz de establecimiento de conexión de salida
configuración 456
mandatos de configuración 458
mandatos de configuración global 463
mandatos de supervisión global 472
protocolo de configuración dinámica de sistemas principales (DHCP)
configuración básica 460
descripción 459
red de varios servidores 461
varios saltos para acceder al servidor 461
requisitos 453
servidor de nombres de dominio dinámico (DDNS)
descripción 461
utilización 451
diffserv
configuración 392, 395
función, resumen 389
indicador de configuración
acceso 395
diffserv *(continuación)*
indicador de supervisión
acceso 400
mandatos de configuración
delete 396
disable 396
enable 396
list 397
resumen 395
set 398
mandatos de supervisión 401
clear 401
dscache 401
list 402
terminología 392
visión general 389
disable
mandato de configuración de la reserva de ancho de banda 41
mandato de configuración de la restauración de WAN 79, 86
mandato de configuración de seguridad IP 365
mandato de configuración del filtrado MAC 62
mandato de conversión de direcciones de red 443
mandato de supervisión de Host On-Demand Client Cache 161
mandato de supervisión de la Antememoria de servidor Web 218
mandato de supervisión de seguridad IP 382
mandato de supervisión del filtrado MAC 68
mandato NAT 443
mandatos de configuración del servidor DHCP 524
mandatos de supervisión del servidor DHCP 542
disable-hpr-over-ip-port-numbers
mandato de configuración de la reserva de ancho de banda 41
DLSw
filtros MAC 55

E

ECP, cifrado
configurar
para PPP 271
ejecutor
para network dispatcher 106

enable
mandato de configuración de conversión de direcciones de red 443
mandato de configuración de la reserva de ancho de banda 41
mandato de configuración de la restauración de WAN 80
mandato de configuración de seguridad IP 366
mandato de configuración del filtrado MAC 62
mandato de configuración NAT 443
mandato de supervisión de Host On-Demand Client Cache 160
mandato de supervisión de la Antememoria de servidor Web 217
mandato de supervisión de la restauración de WAN 87
mandato de supervisión de seguridad IP 383
mandato de supervisión del filtrado MAC 68
mandatos de configuración del servidor DHCP 525
mandatos de supervisión del servidor DHCP 542
enable-hpr-over-ip-port-numbers
mandato de configuración de la reserva de ancho de banda 42
encapsulator PPP
valores por omisión de parámetros
para interfaces de establecimiento de conexión de entrada 455
encontrada petición hecha a la antememoria 172
enlaces Frame Relay
configuración y supervisión de la compresión de datos 239
enlaces PPP
configuración y supervisión de la compresión de datos 236
entorno de supervisión del VCRM
acceso 575
ES
configuración 223
supervisión 223
ESP 339
establecimiento de conexión de entrada
mandatos de supervisión de interfaces 476
establecimiento de conexión de salida
mandatos de configuración de interfaces 476
mandatos de supervisión de interfaces 476

F

filtrado
direccionamiento de multidifusión 7
direcciones MAC 7
orden de precedencia 12
filtrado MAC
acceso al indicador de configuración 59
acceso al indicador de supervisión 67
configuración 59
mandatos secundarios de actualización 57
parámetros 56
utilización de identificadores 57
filtros
y reserva de ancho de banda 7
filtros de paquetes para NAT 436
filtros MAC
discusión 55
para tráfico DLSw 55
flush
mandato de supervisión de la TSF 570
formato de un subcampo
subcampo dependencia 198
subcampo nombre 198
subcampo objeto 198
subcampo petición de contraseña 199
subcampo petición de URL 199
formato de un subvector 183
subvector de mandatos consulta 189
subvector de mandatos depuración 189
subvector de mandatos estadísticas 189
subvector de mandatos máscara de URL 190
subvector de mandatos política 186
subvector de respuesta añadir objeto 190
subvector de respuesta añadir objeto (obligatoriamente) 191
subvector de respuesta consulta 195
formato de un subvector *(continuación)*
subvector de respuesta dependencia 191
subvector de respuesta depuración 195
subvector de respuesta eliminar objeto 191
subvector de respuesta habilitar 192
subvector de respuesta inhabilitar 192
subvector de respuesta máscara de URL 197
subvector de respuesta política 192
formatos de los subcampos 197
formatos de los subvectores
subvector de mandatos añadir objeto 184
subvector de mandatos añadir objeto (obligatoriamente) 184
subvector de mandatos dependencia 184
subvector de mandatos eliminar objeto 184
subvector de mandatos habilitar 186
subvector de mandatos inhabilitar 186
Formatos de los vectores del protocolo de control de la antememoria externa (ECCP) 179
descripciones de los campos 179
formatos de los subvectores 182
vector de petición de autenticación 180
vector de petición de mandatos 180
vector de respuesta de autenticación 181
vector de respuesta de mandatos 181
Frame Relay
cifrado 271
configurar 274
supervisar 274
Reserva de ancho de banda 3
funciones
filtrado MAC 59
filtros MAC 55
supervisión 25
Thin Server Feature (TSF) 547
funciones de conexión por puentes
filtrado MAC 59

funciones de conexión por puentes *(continuación)*
mandatos de actualización 63
mandatos secundarios de actualización 57

G

gestor
para network dispatcher 107
Gestor de control de antememoria externa
añadir un objeto 177
consultar un objeto 178
depurar la partición 178
descripciones 177
inhabilitar y habilitar una partición 178
suprimir un objeto 177
utilización de la tabla de dependencias 177
utilización de las estadísticas 178
utilización de las políticas 178
utilización de una máscara de URL 178
Gestor de recursos de circuito virtual (VCRM)
configuración y supervisión 575

H

Host On-Demand Client Cache
configuración y supervisión 151
definición de un cluster 118

I

identificación de seguridad
descripción 250
limitaciones 251
indicador de configuración de la autenticación
acceder 253
Infraestructura de claves públicas 347
acceso al entorno (IPv4) 377
configuración 354
configuración de la Infraestructura de claves públicas 348
configurar 348
mandatos de configuración 355
add server 355
change server 355
delete certificate 356
Infraestructura de claves públicas *(continuación)*
mandatos de configuración *(continuación)*
delete private-key 356
delete server 356
list certificates 357
list private-keys 357
list servers 357
mandatos de supervisión 378
acceso (IPv4) 377
cert-load (IPv4) 378
cert-req (IPv4) 378
cert-save (IPv4) 379
list certificate (IPv4) 379
list configured-servers (IPv4) 380
load certificate (IPv4) 380
Intercambio de claves de Internet 345
configuración de la Infraestructura de claves públicas 348
fases del intercambio de claves 345
mandatos de supervisión acceso (IPv4) 375
mandatos de supervisión (IPv4) 375
mensaje, intercambios 346
intercambio de claves en Internet
configuración 353
interface
mandato de configuración de la reserva de ancho de banda 43
mandato de supervisión de la reserva de ancho de banda 53
interfaces de establecimiento de conexión de entrada
valores por omisión de encapsulator PPP 455
valores por omisión de parámetros de circuitos de establecimiento de conexión 454
interfaz de establecimiento de conexión de entrada
adición 455
configuración 453
interfaz de establecimiento de conexión de salida
agrupaciones de módems 457
configuración 456
IP, seguridad 335
algoritmos (IPv6) 370
asociación de seguridad (SA) 340
IP, seguridad *(continuación)*
cabecera de autenticación (AH) 338
carga útil de seguridad de encapsulación (ESP) 339
certificado
obtención 354
conceptos 336
configuración (IPv6) 369
configuración de claves (IPv6) 370
configuración de las claves de cifrado (IPv4) 359
configuración de los algoritmos (IPv4) 358
configuración de los algoritmos (IPv6) 370
configuración y supervisión 353
Infraestructura de claves públicas 347
configuración 354
mandatos de configuración 355
mandatos de supervisión 378
Intercambio de claves de Internet 345, 348
intercambio de claves en Internet
configuración 353
mandatos de supervisión (IPv4) 375
jerarquizar protocolos 342
mandatos de configuración
acceso (IPv4) 359
acceso (IPv6) 370
add server 355
add tunnel 359
change server 355
change tunnel 364
delete 356
delete private-key 356
delete server 356
delete tunnel 365
disable 365
enable 366
list 366
list certificates 357
list private-keys 357
list servers 357
set 367
mandatos de supervisión
acceso (IPv4) 381
acceso (IPv6) 387
change tunnel 381
delete 376
delete tunnel 382
disable 382

IP, seguridad *(continuación)*
mandatos de supervisión *(continuación)*
enable 383
list 376, 383
reset 385
set 386
stats 377, 386
mandatos de supervisión (IPv4) 381
mandatos de supervisión (IPv6) 387
manual
configuración (IPv4) 358
supervisión (IPv4) 387
manual (IPv4) 352
manual (IPv6) 352
negociado 345
mensaje, intercambios 346
preparación para operaciones negociadas de seguridad IP 353
supervisión (IPv4) 375
supervisión (IPv6) 387
supervisión de intercambio de claves en Internet (IPv4) 375
terminología 336
transporte, modalidad 340
túnel
diagrama de red 344
túnel en túnel 342
túnel manual
configuración (IPv4) 368
configuración (IPv6) 371
túnel, modalidad 340
túneles protegidos 335
utilizar 335
AH y ESP 339
vía de acceso, descubrimiento de la MTU 343
visión general 335
y paquetes L2TP 342

L

L2F
configuración 417
L2T 407
configuración 410
consideraciones
LCP 410
tiempo 410
funciones que reciben soporte 408
mandatos de configuración
add 420
disable 418, 420
enable 418, 421
encapsulator 418, 422
L2T *(continuación)*
mandatos de configuración *(continuación)*
list 418, 422
resumen 417, 419
set 418, 423
terminología 408
visión general 407
L2TP
configuración 417
mandatos de supervisión 425
call 425
kill 428
memory 428
start 428
stop 428
tunnel 429
L2TP, paquetes
y seguridad IP 342
last
mandato de supervisión de la reserva de ancho de banda 54
last-circuit-class
mandato de supervisión de la reserva de ancho de banda 54
LDAP
configurar 311
mandatos de configuración
disable 325
enable 325
resumen 325
set 327
set default-policy 325
set refresh 328
list
mandato de actualización del filtrado MAC 65
mandato de configuración de conversión de direcciones de red 443
mandato de configuración de Host On-Demand Client Cache 157
mandato de configuración de la Antememoria de servidor Web 210
mandato de configuración de la característica de voz 591
mandato de configuración de la reserva de ancho de banda 44
mandato de configuración de la restauración de WAN 81
mandato de configuración de la TSF 566
mandato de configuración de seguridad IP 366
list *(continuación)*
mandato de configuración del filtrado MAC 62
mandato de configuración del puerto de voz 597
mandato de configuración NAT 443
mandato de supervisión de Host On-Demand Client Cache 161
mandato de supervisión de la Antememoria de servidor Web 218
mandato de supervisión de la restauración de WAN 91
mandato de supervisión de la TSF 570
mandato de supervisión de NAT 449
mandato de supervisión de seguridad IP 376, 383
mandato de supervisión del filtrado MAC 68
mandatos de configuración del servidor DHCP 525, 542
mandatos de supervisión de la conversión de direcciones de red 449
parámetros del subsistema de codificación (talk 5) 226
parámetros del subsistema de codificación (talk 6) 224
list certificate
mandato de supervisión de PKI (IPv4) 379
list certificates
mandato de configuración de seguridad IP 357
list configured-servers
mandato de supervisión de PKI (IPv4) 380
list private-keys
mandato de configuración de seguridad IP 357
list servers
mandato de configuración de seguridad IP 357
load certificate
mandato de supervisión de PKI (IPv4) 380

M

mandato de supervisión del VCRM
clear 576
queue 576
mandato dials 463

mandato feature 559
mandato list devices 587
mandatos
DIALs
configuración global 463
supervisión global 472
establecimiento de conexión de entrada
supervisión de interfaces 476
establecimiento de conexión de salida
configuración de interfaz 476
supervisión de interfaces 476
mandatos de configuración 353
autenticación 253
default-policy
set 325
DIALs 458
diffserv 395
delete 396
disable 396
enable 396
list 397
set 398
global de DIALs 463
interfaz de establecimiento de conexión de salida 476
IPSec 353
acceso (IPv4) 359
acceso (IPv6) 370
add server 355
add tunnel 359
change server 355
change tunnel 364
delete certificate 356
delete private-key 356
delete server 356
delete tunnel (IPv4) 365
disable 365
enable 366
list 366
list certificates 357
list private-keys 357
list servers 357
set 367
L2F, resumen de 417, 419
L2T
add 420
disable 418, 420
enable 418, 421
L2TP
call 425
encapsulator 418, 422
kill 428
list 418, 422
memory 428
mandatos de configuración *(continuación)*
L2TP *(continuación)*
start 428
stop 428
tunnel 429
L2TP, resumen de 417, 419
LDAP 325
disable 325
enable 325
set 327
política 311
add 311
copy 324
change 324
delete 324
disable 324
enable 324
list 324
PPTP, resumen de 417, 419
refresh
set 328
túnel
add 420
túneles L2
set 418, 423
Mandatos de configuración de conversión de direcciones de red
list 443
mandatos de configuración de Host On-Demand Client Cache
activate 156
add 156
delete 156
list 157
modify 158
mandatos de configuración de interfaces
establecimiento de conexión de salida 476
mandatos de configuración de la Antememoria de servidor Web
activate 208
add 208
delete 209
list 210
modify 211
mandatos de configuración de la característica de voz
acceso 587
add 588
delete 591
list 591
modify 593
reorder-call-rule 593
set 593
Mandatos de configuración de la conversión de direcciones de red 441
mandatos de configuración de la Reserva de ancho de banda
acceso al indicador de configuración de BRS 25
activate-ip-precedence-filtering 30
add-circuit-class 31
add-class 31
assign 33
assign-circuit 36
circuit 37
clear-block 38
configuración de ejemplo 13
create-super-class 38
change-circuit-class 37
change-class 37
deactivate-ip-precedence-filtering 39
deassign 39
deassign-circuit 39
default-circuit-class 39
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 47
show 48
tag 48
untag 49
use circuit defaults 49
mandatos de configuración de la restauración de WAN
add 78
disable 79
enable 80
list 81
remove 81
resumen 77
mandatos de configuración de la tsf
add 559
delete 565
list 566
modify 566
resumen 559
set 567
Mandatos de configuración de NAT 441
mandatos de configuración de una red de voz
acceso 597
mandatos de configuración del filtrado MAC

mandatos de configuración del filtrado MAC *(continuación)*
acceso 59
attach 60
create 60
default 60
delete 61
detach 61
disable 62
enable 62
list 62
mandatos de actualización
add 64
delete 65
list 65
move 66
resumen 63
set-action 66
mandatos secundarios de actualización 57
move 63
reinit 63
resumen 59
set-cache 63
update 63
mandatos de configuración del puerto de voz
list 597
set 598
mandatos de configuración del redireccionamiento de WAN
set 82, 88
mandatos de configuración del servidor DHCP
acceso 509
add 510
change 516
delete 521
disable 524
enable 525
list 525, 542
set 532
mandatos de configuración global DIALs 463
mandatos de conversión de direcciones de red
change 442
delete 442
disable 443
enable 443
map 444
reserve 445
reset 447
set 447
Mandatos de la Antememoria de servidor Web 208
mandatos de modificación de Host On-Demand Client Cache
mandatos de modificación de Host On-Demand Client Cache *(continuación)*
modify 163
mandatos de modificación de la Antememoria de servidor Web
modify 221
mandatos de supervisión
diffserv
clear 401
dscache 401
list 402
global de DIALs 472
interfaz de establecimiento de conexión de entrada 476
interfaz de establecimiento de conexión de salida 476
IPSec 353
change tunnel 381
delete 376
delete tunnel 382
disable 382
enable 383
IKE, acceso (IPv4) 375
IPSec, acceso (IPv4) 381
IPSec, acceso (IPv6) 387
list 376, 383
PKI, acceso (IPv4) 377
reset 385
set 386
stats 377, 386
mandatos de supervisión de DIALS
acceso 472
mandatos de supervisión de Host On-Demand Client Cache
activate 159
clear 160
delete 160
disable 161
enable 160
list 161
mandatos de supervisión de interfaces
establecimiento de conexión de entrada 476
establecimiento de conexión de salida 476
mandatos de supervisión de la Antememoria de servidor Web
activate 216
clear 216
delete 217
disable 218
enable 217
list 218
mandatos de supervisión de la reserva de ancho de banda
mandatos de supervisión de la reserva de ancho de banda *(continuación)*
acceso al indicador de supervisión 50
circuit 51
clear 52
clear-circuit-class 52
counters 52
counters-circuit-class 53
interface 53
last 54
last-circuit-class 54
resumen 50
mandatos de supervisión de la restauración de WAN
acceso 85
clear 86
disable 86
enable 87
list 91
resumen 85
mandatos de supervisión de la TSF
acceso 569
archivo 570
delete-file 569
flush 570
refresh 573
reset 574
restart 574
resumen de 569
set 574
mandatos de supervisión del adaptador de voz
acceso 600
calls 601
resumen 600
status 602
trace 604
mandatos de supervisión del filtrado MAC
acceso 67
clear 67
disable 68
enable 68
list 68
reinit 69
resumen 67
mandatos de supervisión del servidor DHCP
acceso 541
disable 542
enable 542
request 543
reset 542
mandatos de supervisión global DIALs 472

mandatos NAT
change 442
delete 442
disable 443
enable 443
list 443
map 444
reserve 445
reset 447
set 447
mandatos secundarios de actualización
mandato de configuración del filtrado MAC 57
manual, seguridad IP
IPv4 352
IPv6 352
map
mandato de configuración de conversión de direcciones de red 444
mandato de configuración NAT 444
marcación por desbordamiento 71
modify
mandato de configuración de Host On-Demand Client Cache 158
mandato de configuración de la Antememoria de servidor Web 211
mandato de configuración de la característica de voz 593
mandato de configuración de la TSF 566
mandato de modificación de Host On-Demand Client Cache 163
mandato de modificación de la Antememoria de servidor Web 221
move
mandato de actualización del filtrado MAC 66
mandato de configuración del filtrado MAC 63
MPPE
configurar 271
para PPP 272
multiplexor Nuera F200
configuración 580

N

NAPT
utilización 434
NAT
configuración 441
correlaciones de direcciones estáticas 435
ejemplo de configuración 436
filtros de paquetes 436
mandatos de supervisión 448
reglas de control de acceso 436
utilización 433
negociado, seguridad IP 345
fases del intercambio de claves IKE 345
IKE, intercambios de mensajes 346
mensaje, intercambios 346
operaciones
preparación para 353
network dispatcher 105
alta disponibilidad 107
aplicaciones de gestión SNMP 106
asesores 106
configuración 109
ejecutor 106
gestor 107
mandato de configuración 105, 121
acceso 121, 140
add 121
clear 128
disable 128
enable 129
list 131, 141
quiesce 143
remove 132
report 144
resumen de 121, 141
set 135
status 145
reparto de carga 106
utilización 105
pasos 111
visión general 105
network dispatcher con Antememoria de servidor Web y con acierto en la antememoria 167
network dispatcher con Antememoria de servidor Web y sin acierto en la antememoria 166
network dispatcher sin Antememoria de servidor Web 166
Network Station 547
NSF
utilización de TFTP 550

P

palabras clave 605
parámetros
filtrado MAC 56
petición reenviada a la antememoria responsable 173
petición reenviada a la antememoria responsable y no encontrada 174
petición reenviada al servidor final 173
plan de marcación (Nuera F200) 582
política
configuración, ejemplos 288
configurar 311
decisión y aplicación 275
decisión y flujo de datos 276
desconectar todo el tráfico público 303
esquema 285
función, resumen 275
generar normas 287
IKE, decisiones 277
indicador de configuración
acceder 311
Interacción de la base de datos de políticas y LDAP 283
IP, consultas 277
IPSec, consultas 277
LDAP, motor de búsqueda de políticas
configurar y habilitar 307
mandatos de configuración
add 311
copy 324
change 324
delete 324
disable 324
enable 324
list 324
resumen 311
objetos 278
Política de sólo IPSec/ISAKMP 300
Política IPSec/ISAKMP con QOS 288
RSVP, decisiones 278
supervisar, indicador
acceder 329
supervisar, mandatos 329
disable 329
enable 330
list 331
reset 330
search 330
status 330
test 332

política *(continuación)*
visión general 275
PPTP
configuración 417
preparación para operaciones negociadas de seguridad IP 353
protocolo de configuración dinámica de sistemas principales (DHCP)
configuración básica 460
descripción 459
red de varios servidores 461
varios saltos para acceder al servidor 461
Protocolo de control de la antememoria externa 176
configuración 176
Protocolo de control del cifrado para PPP 271
Protocolo punto a punto (PPP)
Protocolo de control del cifrado 271
protocolos
adaptador de voz 587
Protocolos de control de la red (NCP)
para interfaces PPP
Protocolo de control del cifrado 271

Q

queue
mandato de supervisión del VCRM 576
queue-length
mandato de configuración de la reserva de ancho de banda 47

R

radius 605
redireccionamiento de WAN
asignación del enlace alternativo 102
configuración 99
configuración de circuitos de marcación 102
configuración de ejemplo 99
configuración de Frame Relay 101
configuración de RDSI 102
configuración del enlace alternativo 102
discusión 97
visión general 71
refresh
mandato de supervisión de la TSF 573
reglas de control de acceso para NAT 436
reinit
mandato de configuración del filtrado MAC 63
mandato de supervisión del filtrado MAC 69
remove
mandato de configuración de la restauración de WAN 81
reorder-call-rule
mandato de configuración de la característica de voz 593
reparto de carga
con network dispatcher 106
request
mandatos de supervisión del servidor DHCP 543
requisitos
para dial-in-access server 453
reserva de ancho de banda
acceso a los indicadores de supervisión 50
acceso al indicador de configuración 25
con filtros 7
configuración 1
mandatos de configuración resumen 28
sobre Frame Relay 3
reserve
mandato de conversión de direcciones de red 445
mandato NAT 445
reset
configuración de la conversión de direcciones de red 450
mandato de configuración de conversión de direcciones de red 447
mandato de configuración NAT 447, 450
mandato de supervisión de la TSF 574
mandato de supervisión de seguridad IP 385
mandatos de supervisión del servidor DHCP 542
restart
mandato de supervisión de la TSF 574
restauración de WAN
configuración del circuito de marcación secundario 74
procedimiento de configuración 74
restauración de WAN *(continuación)*
visión general 71

S

seguridad 176
autenticación 245
autorización 245
contabilidad 245
seguridad AAA
seguridad 245
seguridad IP manual 353
mandatos de configuración (IPv4) 359
supervisión (IPv6) 387
servicio de nombres de dominio dinámico (DDNS)
descripción 461
servidor
ACE/Server
limitaciones 251
soporte 250
autenticación
definición 249
DIALs
definición 451
mandatos de configuración 458
requisitos 453
utilización 451
Servidor BOOTP 483
servidor de autenticación
ACE/Server 250
definición 249
servidor DHCP 479, 509
clientes DHCP especiales 483
conceptos 484
ejemplo de configuración 501
introducción 479
movimiento del cliente 481
número de servidores DHCP 482
opciones
base, proporcionadas al cliente 489
específicas de IBM 499
extensiones DHCP 495
formatos 487
parámetro de aplicaciones y servicios 494
parámetros de capa de enlace por opciones de interfaz 493
parámetros de capa IP por opciones de interfaz 492
parámetros de capa IP por opciones de sistema principal 491

servidor DHCP *(continuación)*
opciones *(continuación)*
parámetros TCP 493
proveedor 499
opciones de servidor, modificación 481
operación DHCP 479
parámetros de servidor DHCP y de cesión 487
renovaciones de cesiones 481
servidor DHCP, único 482
servidor DHCP, varios 482
Servidores BOOTP 483
terminología 484
tiempos de cesión 484
servidor TN3270E 151
set
mandato de configuración de conversión de direcciones de red 447
mandato de configuración de la característica de voz 593
mandato de configuración de la TSF 567
mandato de configuración de seguridad IP 367
mandato de configuración del puerto de voz 598
mandato de configuración del redireccionamiento de WAN 82, 88
mandato de configuración NAT 447
mandato de supervisión de la TSF 574
mandato de supervisión de seguridad IP 386
mandatos de configuración del servidor DHCP 532
parámetros del subsistema de codificación 225
set circuit defaults
mandato de configuración de la reserva de ancho de banda 47
set-action
mandato de actualización del filtrado MAC 66
show
mandato de configuración de la reserva de ancho de banda 48
Sistema de reserva de ancho de banda (BRS)
descripción 1
Elegibilidad para ser descartado (DE) 4
Filtrado de número de puerto TCP/UDP 8
Sistema de reserva de ancho de banda (BRS) *(continuación)*
proceso de bits de precedencia de IP versión 4 10
stats
mandato de supervisión de seguridad IP 377, 386
status
mandato de supervisión del adaptador de voz 602
subsistema de codificación
configuración 223
supervisión 223, 225
supervisar
cifrado
para Frame Relay 274
para PPP 272
MPPE
para PPP 273
supervisar, mandatos
política
disable 329
enable 330
list 331
reset 330
search 330
status 330
test 332
supervisión 353
compresión de datos para enlaces Frame Relay 239
compresión de datos para enlaces PPP 236
mandatos de supervisión de la TSF 569
mandatos de supervisión del adaptador de voz 600
seguridad IP (IPv4) 375
seguridad IP manual (IPv6) 387

T

tabla de dependencias 175
TACACS 606
tag
mandato de configuración de la reserva de ancho de banda 48
talk
mandato OPCON 463, 472, 509, 541, 559, 569, 587, 600
thin server function
configuración 559
trace
mandato de supervisión del adaptador de voz 604
translate
mandato de configuración de conversión de direcciones de red 448
mandato de configuración NAT 448
transporte, modalidad 340
TSF
actualizaciones de antememorias de archivos 551
configuración 559
configuración del servidor BootP/DHCP 552
configuración del servidor para TSF 553
ejemplo de configuración 553
pasos de configuración 551
utilización 547
utilización de RFS 550
utilización de TFTP 550
visión general 547
túnel en túnel para la seguridad IP 342
túnel, modalidad 340
túneles protegidos 335

U

untag
mandato de configuración de la reserva de ancho de banda 49
update
mandato de configuración del filtrado MAC 63
use circuit defaults
mandato de configuración de la reserva de ancho de banda 49
utilización
dial-in access server 451
utilización de la Antememoria de servidor Web 165
utilización de la restauración de WAN 71
utilización del Proxy HTTP 170

V

VCRM
configuración y supervisión 575
Vector de respuesta de mandatos 179
vía de acceso, descubrimiento de la MTU 343

visión general
de la compresión 231
redireccionamiento de WAN 71
restauración de WAN 71
Visión general de la Antememoria de servidor Web 165
Visión general del gestor de control de antememoria externa 174
voz
mandatos de configuración, resumen 587
voz sobre Frame Relay (VOFR) 33

Hoja de Comentarios

Access Integration Services
Utilización y configuración
de las características
Versión 3.3

Número de Publicación SC10-3437-00

En general, ¿está Ud. satisfecho con la información de este libro?

	Muy satisfecho	Satisfecho	Normal	Insatisfecho	Muy insatisfecho
Satisfacción general	□	□	□	□	□

¿Cómo valora los siguientes aspectos de este libro?

	Muy bien	Bien	Acep-table	Insatisfecho	Muy insatisfecho
Organización	□	□	□	□	□
Información completa y precisa	□	□	□	□	□
Información fácil de encontrar	□	□	□	□	□
Utilidad de las ilustraciones	□	□	□	□	□
Claridad de la redacción	□	□	□	□	□
Calidad de la edición	□	□	□	□	□
Adaptación a los formatos, unidades, etc. del país	□	□	□	□	□

Comentarios y sugerencias:

Nombre

Dirección

Compañía u Organización

Teléfono

Hoja de Comentarios
SC10-3437-00

Corte o Doble
Por la Línea

Dóblese por la línea de puntos **Por favor no lo grape** Dóblese por la línea de puntos

PONER
EL
SELLO
AQUÍ

IBM, S.A.
National Language Solutions Center
Av. Diagonal, 571
08029 Barcelona
España

Dóblese por la línea de puntos **Por favor no lo grape** Dóblese por la línea de puntos

SC10-3437-00

Corte o Doble
Por la Línea

Printed in Denmark by IBM Danmark A/S

SC10-3437-00